

## НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

### HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологичных космических исследований Земли.

**Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссией России (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.**

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:

- 05.07.00 Авиационная и ракетно-космическая техника
- 05.12.00 Радиотехника и связь
- 05.13.00 Информатика, вычислительная техника и управление.

#### ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

- NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Все номера журнала находятся в свободном доступе на сайте журнала [www.hes.ru](http://www.hes.ru) и библиотеке [elibrary.ru](http://elibrary.ru).

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: [HT-ESResearch@yandex.ru](mailto:HT-ESResearch@yandex.ru). С требованиями можно ознакомиться на сайте: [www.H-ES.ru](http://www.H-ES.ru).

Язык публикаций: русский, английский.  
Периодичность выхода – 6 номеров в год.  
Свидетельство о регистрации СМИ ПИ № ФС 77-60899 от 02.03.2015  
Территория распространения: Российская Федерация, зарубежные страны

Тираж 1000 экз. Цена 1000 руб.  
Плата с аспирантов за публикацию рукописи не взимается.

© ООО «ИД Медиа Паблишер», 2021

**H&ES Research** is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

**The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.**

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the Nomenclature of specialties:

- 05.07.00 Aviation, space-rocket hardware
- 05.12.00 RF technology and communication
- 05.13.00 Informatics, computer engineering and control.

#### JOURNAL H&ES RESEARCH INDEXING

All issues of the journal are in a free access on a site of the journal [www.hes.ru](http://www.hes.ru) and [elibrary.ru](http://elibrary.ru).

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: [HT-ESResearch@yandex.ru](mailto:HT-ESResearch@yandex.ru). The requirements are available on the website: [www.H-ES.ru](http://www.H-ES.ru).

Language of publications: Russian, English.  
Periodicity – 6 issues per year.  
Media Registration Certificate PI No. FS77-60899. Date of issue: March 2, 2015.  
Distribution Territory: Russian Federation, foreign countries

Circulation of 1000 copies. Price of 1000 Rub.  
Postgraduate students for publication of the manuscript will not be charged

© "Media Publisher", LLC 2021

5  
2021  
T.13

## СОДЕРЖАНИЕ

### Учредитель:

ООО "ИД Медиа Паблишер"

### Издатель:

ДЫМКОВА С.С.

### Главный редактор:

ЛЕГКОВ К.Е.

### Редакционная коллегия:

**БОБРОВСКИЙ В.И.**, д.т.н., доцент;  
**БОРИСОВ В.В.**, д.т.н., профессор,  
Действительный член академии военных наук РФ;

**БУДКО П.А.**, д.т.н., профессор;

**БУДНИКОВ С.А.**, д.т.н., доцент,

Действительный член Академии

информатизации образования;

**ВЕРХОВА Г.В.**, д.т.н., профессор;

**ГОНЧАРОВСКИЙ В.С.**, д.т.н.,

профессор, заслуженный деятель науки и техники РФ;

**КОМАШИНСКИЙ В.И.**, д.т.н., профессор;

**КИРПАНЕВ А.В.**, д.т.н., доцент;

**КУРНОСОВ В.И.**, д.т.н., профессор,

академик Международной академии

информатизации, Действительный член

Российской академии естественных наук;

**МОРОЗОВ А.В.**, д.т.н., профессор,

Действительный член Академии военных наук РФ;

**МОШАК Н.Н.**, д.т.н., доцент;

**ПАВЛОВ А.Н.**, д.т.н., профессор;

**ПРОРОК В.Я.**, д.т.н., профессор;

**СЕМЕНОВ С.С.**, д.т.н., доцент;

**СИНИЦЫН Е.А.**, д.т.н., профессор;

**ШАТРАКОВ Ю.Г.**, д.т.н., профессор,

заслуженный деятель науки РФ.

### Адрес издателя:

111024, Россия, Москва,  
ул. Авиамоторная, д. 8, корп. 1, офис 323.

### Адрес редакции:

194044, Россия, Санкт-Петербург,  
Лесной Проспект, 34-36, к. 1,  
Тел.: +7(911) 194-12-42.

### Адрес типографии:

Россия, Москва, ул. Складочная, д. 3,  
кор. 6.

Мнения авторов не всегда совпадают с точкой зрения редакции.

За содержание рекламных материалов редакция ответственности не несет.

Материалы, опубликованные в журнале – собственность ООО "ИД Медиа Паблишер".

Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя.

### АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

**Морозов Д.А., Кузнецов Д.А.,  
Леве Д.Е., Перминов А.Ю.**

Проектирование автоматизированной системы пространственных смещений фазового центра спутниковой геодезической аппаратуры

4

### РАДИОТЕХНИКА И СВЯЗЬ

**Аллакин В.В.**

Методика превентивной идентификации состояния объектов мониторинга на основе символического представления временных рядов их метрик

13

**Багрецов С.А., Галкин И.А.,  
Ачкасов Н.Б., Иванов Д.А.**

Методика анализа построения структурного резервирования информационно-телекоммуникационной сети в условиях воздействия противника

29

**Будко Н.П.**

Методика синтеза подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети ситуационного центра

38

**Аджемов С.С., Лобов Е.М., Кандауров Н.А.,  
Лобова Е.О., Липаткин В.И.**

Алгоритмы оценки и компенсации дисперсионных искажений широкополосных сигналов ионосферных радиолиний связи

57

### ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

**Коржик В.И., Нгуен З.К., Даньшина А.В.**

Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения

75

**Крюкова Е.С., Ткаченко В.В.,  
Михайличенко А.В., Паращук И.Б.**

Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров

86

**Митрофанов М.В., Крибель А.М.,  
Фроленков А.С., Спицын О.Л.**

Методика обнаружения атак, типа SQL-инъекция на основе алгоритмов искусственного интеллекта, методом задачи классификации

96



# CONTENTS

## AVIATION, SPACE-ROCKET HARDWARE

**Morozov D.A., Kuznetsov D.A.,  
Leve D.E., Perminov A.Yu.**

Design of an automated system of spatial displacements  
of the phase center of satellite geodetic equipment

4

## RF TECHNOLOGY AND COMMUNICATION

**Allakin V.V.**

The method of preventive identification of the state  
of monitoring objects based on the symbolic representation  
of time series of their metrics

13

**Bagretsov S.A., Galkin I.A.,  
Achkasov N.B., Ivanov D.A.**

Methodology for analyzing the construction of structural  
redundancy of an information and telecommunications network  
under the influence of the enemy

29

**Budko N.P.**

The method of synthesis of the subsystem of intelligent  
monitoring of the information and telecommunications  
network of the situation center

38

**Adjemov S.S., Lobov E.M., Kandaurov N.A.,  
Lobova E.O., Lipatkin V.I.**

Algorithms of estimating and compensating the dispersion  
distortions of wideband signals in the HF channel

57

## INFORMATICS, COMPUTER ENGINEERING AND CONTROL

**Korzhik V.I., Nguen Z.K., Danshina A.V.**

Detection of stegosystem using embedding into contours  
of images

75

**Kryukova E.S., Tkachenko V.V.,  
Mikhailichenko A.V., Parashchuk I.B.**

Questions of reliability assessment of modern data storage  
systems for mobile data centers

86

**Mitrofanov M.V., Kribel A.M.,  
Frolenkov A.S., Spitsyn O.L.**

The method of detecting attacks, such as SQL-injection  
based on artificial intelligence algorithms, by the method  
of the classification problem

96

### Founder:

"Media Publisher", LLC

### Publisher:

DYMKOVA S.S.

### Editor in chief:

LEGKOV K.E.

### Editorial board:

**BOBROWSKY V.I.**, PhD, Docent;  
**BORISOV V.V.**, PhD, Full Professor;  
**BUDKO P.A.**, PhD, Full Professor;  
**BUDNIKOV S.A.**, PhD, Docent,  
Actual Member of the Academy of  
Education Informatization;  
**VERHOVA G.V.**, PhD, Full Professor;  
**GONCHAREVSKY V.S.**, PhD, Full  
Professor, Honored Worker of Science  
and Technology of the Russian Federation;  
**KOMASHINSKIY V.I.**, PhD, Full Professor;  
**KIRPANEEV A.V.**, PhD, Docent;  
**KURNOSOV V.I.**, PhD, Full Professor,  
Academician of the International Academy  
of Informatization, law and order, Member  
of the Academy of Natural Sciences;  
**MOROZOV A.V.**, PhD, Full Professor,  
Actual Member of the Academy of Military  
Sciences;  
**MOSHAK N.N.**, PhD, Docent;  
**PAVLOV A.N.**, PhD, Full Professor;  
**PROROK V.Y.**, PhD, Full Professor;  
**SEMENOV S.S.**, PhD, Docent;  
**SINICYN E.A.**, PhD, Full Professor;  
**SHATRAKOV Y.G.**, PhD, Full Professor;  
Honored Worker of Science of the Russian  
Federation.

### Address of publisher:

111024, Russia, Moscow,  
st. Aviamotornaya, 8, bild. 1, office 323;

### Address of edition:

194044, Russia, St. Petersburg,  
Lesnoy av., 34-36, h.1,  
Phone: +7 (911) 194-12-42.

### Address of printing house:

Russia, Moscow, st. Skladochnaya, 3, h. 6

The opinions of the authors don't always  
coincide with the point of view of the pub-  
lisher. For the content of ads, the editorial  
Board is not responsible. All articles and  
illustrations are copyright. All rights  
reserved. No reproduction is permitted in  
whole or part without the express consent of  
Media Publisher Joint-Stock company.

doi: 10.36724/2409-5419-2021-13-5-4-12

# ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРОСТРАНСТВЕННЫХ СМЕЩЕНИЙ ФАЗОВОГО ЦЕНТРА СПУТНИКОВОЙ ГЕОДЕЗИЧЕСКОЙ АППАРАТУРЫ

**МОРОЗОВ**

**Дмитрий Андреевич<sup>1</sup>**

**КУЗНЕЦОВ**

**Дмитрий Александрович<sup>2</sup>**

**ЛЕВЕ**

**Дмитрий Евгеньевич<sup>3</sup>**

**ПЕРМИНОВ**

**Алексей Юрьевич<sup>4</sup>**

## АННОТАЦИЯ

**Введение:** Для оценки точности определения координат, получаемых различными методами позиционирования и технологиями обработки данных, используются специальные экспериментальные установки – системы пространственных смещений фазового центра антенны. В работе рассматривается проектирование автоматизированной системы пространственных смещений фазового центра спутниковой геодезической аппаратуры. **Цель исследования:** разработка автоматизированной системы пространственных смещений фазового центра спутниковой геодезической аппаратуры. **Методы:** в процессе работы проводились исследования, направленные на формирование требований к автоматизированной системе пространственных смещений фазового центра, анализ конструкции и назначения существующих систем и разработку системы, отвечающей актуальным требованиям. **Результаты:** представлен анализ отечественного и зарубежного опыта разработки и применения подобных систем, представлена их классификация и выявлены наиболее удачные технические решения. На основании анализа задач, потенциально решаемых системой, разработаны требования к её техническим характеристикам. В соответствии с заданными техническими характеристиками подобрана элементная база и разработана конструкция системы, обеспечивающая антенны приёма сигналов глобальных навигационных спутниковых систем по окружности радиусом от 0 до 500 мм. При этом радиус может динамически изменяться с точностью 0,2 мм. Кроме того, система позволяет изменять положение антенны Глобальных Навигационных Спутниковых Систем по высоте в пределах от 0 до 230 мм с точностью 0,05 мм. Разработанная система не требует постоянного закрепления и может быть перемещена в требуемый район работ. Результаты выполнения работы следует использовать для сборки опытного образца автоматизированной системы пространственных смещений фазового центра спутниковой геодезической аппаратуры. **Практическая значимость:** Разработанная система может быть использована для проведения кинематических испытаний СГА и проведения широкого спектра исследований в рамках моделирования движений опорной спутниковой станции в условиях влияния техногенного и природного характера. **Обсуждение:** Дальнейшее развитие системы может включать в себя определение её метрологических характеристик с применением методов ближней фотограмметрии.

## Сведения об авторах:

<sup>1</sup> преподаватель кафедры Прикладной геодезии, Московский Государственный Университет Геодезии и Картографии, Москва, Россия, dez.data@mail.ru

<sup>2</sup> преподаватель кафедры Прикладной геодезии, Московский Государственный Университет Геодезии и Картографии, Москва, Россия, dmitri-kuznetsov-94@mail.ru

<sup>3</sup> преподаватель кафедры Прикладной геодезии, Московский Государственный Университет Геодезии и Картографии, Москва, Россия, dmleve@yandex.ru

<sup>4</sup> преподаватель кафедры Прикладной геодезии, Московский Государственный Университет Геодезии и Картографии, Москва, Россия, varhood@gmail.com

**КЛЮЧЕВЫЕ СЛОВА:** автоматизированная система, ГНСС, системы смещения фазового центра ГНСС-антенн, спутниковая геодезическая аппаратура.

**Для цитирования:** Морозов Д.А., Кузнецов Д.А., Лева Д.Е., Перминов А.Ю. Проектирование автоматизированной системы пространственных смещений фазового центра спутниковой геодезической аппаратуры // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 4–12. doi: 10.36724/2409-5419-2021-13-5-4-12



## Введение

Системы для контролируемых смещений антенн приёма сигналов глобальных навигационных спутниковых систем (ГНСС) и контроля положения фазового центра спутниковой геодезической аппаратуры (СГА) применяются для:

1) испытания точностных характеристик СГА при позиционировании кинематическими методами («кинематика», «кинематика в реальном времени», PPP-кинематика, метод подвижной базы) в условиях, приближённых к реальным;

2) моделирование реальных движений пункта под влиянием техногенных или природных факторов с целью исследования их влияния на результаты статического позиционирования;

3) исследования и испытания систем мониторинга деформаций, основанных на применении спутниковой геодезической аппаратуры;

4) исследования и испытания технологий определения пространственного положения объектов по результатам обработки измерений, выполненных спутниковой геодезической аппаратурой.

Существующие системы смещения фазового центра СГА имеют различную конструкцию, обеспечивающую круговое движение [1, 3], плановые смещения [1-5] и смещения по высоте [4].

Для проектирования автоматизированной системы пространственных смещений фазового центра СГА был выполнен анализ функциональных возможностей существующих систем. Были рассмотрены отечественные разработки на базе таких организаций, как МИИГАиК [1] и ВНИИФТРИ, и опыт иностранных университетов и организаций [2-5].

По результатам анализа сделаны следующие выводы относительно функционала систем пространственных смещений фазового центра СГА:

1) Рассмотренные системы предназначены для контролируемого перемещения в пространстве одной или двух антенн ГНСС по одному или нескольким следующим основным типам смещений:

- а) Движение по круговой траектории (вращение);
- б) Линейные перемещения в плане;
- в) Линейные перемещения по высоте;
- г) Наклоны относительно вертикальной оси.

2) Движения производятся в соответствии с заданной программой и могут выполняться как с постоянной скоростью, так и с ускорением. В большинстве систем движения производятся автоматизировано.

3) Положение антенны (антенн) определяется в системе координат, связанной с конструкцией либо контролируется только расстояние до оси вращения, и в редких случаях ориентируется в пространстве при помощи угломерных геодезических инструментов.

4) Дополнительные средства измерений для контроля положения антенн или других элементов системы чаще всего не используются;

Смещения, поддерживаемые в каждой из рассмотренных систем, представлены в таблице 1.

Таблица 1

Сводная таблица функционала по типам движения

№ образца	Вращение	Смещение в плане/ число осей	Смещение по высоте	Наклон	Одновременно используемые типы
1	+	-	-	-	-
2	-	+ / 2	-	-	-
3	-	+ / 2	-	-	-
4	+	-	-	-	-
5	-	+ / 1	-	-	-
6	-	+ / 1	+	-	-
7	-	+ / 1	-	-	-
8	+	+ / 1	-	+	+
9	-	+ / 1	+	-	+
10	-	+ / 1	-	-	-
11		-	-	-	-

Данные, представленные в таблице, показывают, что почти все рассмотренные системы реализуют плановые смещения либо по одной, либо по двум осям. Половина из существующих систем позволяют реализовать вращение СГА по определённому радиусу. Смещения по высоте и наклоны СГА реализуются в очень ограниченном количестве систем. В основном, одновременно большинство станций могут выполнять движения только одного типа.

## Требования к проектируемой системе

Использование методов, применяющих технологии ГНСС для мониторинга деформаций, имеет ряд преимуществ, которые делают их эффективными с точки зрения времени и экономической эффективности по сравнению с другими подходами. Пространственное положение точки, находящейся на земной поверхности, изменяется под действием тектонического движения и различных геофизических эффектов, а вектор положения пункта  $\vec{P}(t)$  можно задать в следующем виде:

$$\vec{P}(t) = \vec{P}_0 + V_0 \times (t - t_0) + \sum_i \Delta_i R(t) \quad (1)$$

где:  $\vec{P}_0$  – вектор положения (координаты пункта) на начальную эпоху;  $V_0$  – скорость тектонического движения литосферных плит;  $(t - t_0)$  – промежуток времени между двумя эпохами;  $\Delta_i R(t)$  – поправки за геофизические эффекты.

Автоматизированная система пространственных смещений фазового центра СГА может быть использована для определения величин деформаций положения пункта или объекта под влиянием техногенных и природных факторов. Для этого рассмотрим величины деформационных процессов, для которых может быть применена СГА, чтобы определить требования к автоматизированной системе пространственных смещений фазового центра СГА.

В настоящее время активно начинают развиваться и внедряться технологии, позволяющие использовать СГА для наблюдений за деформационными процессами [6-8].



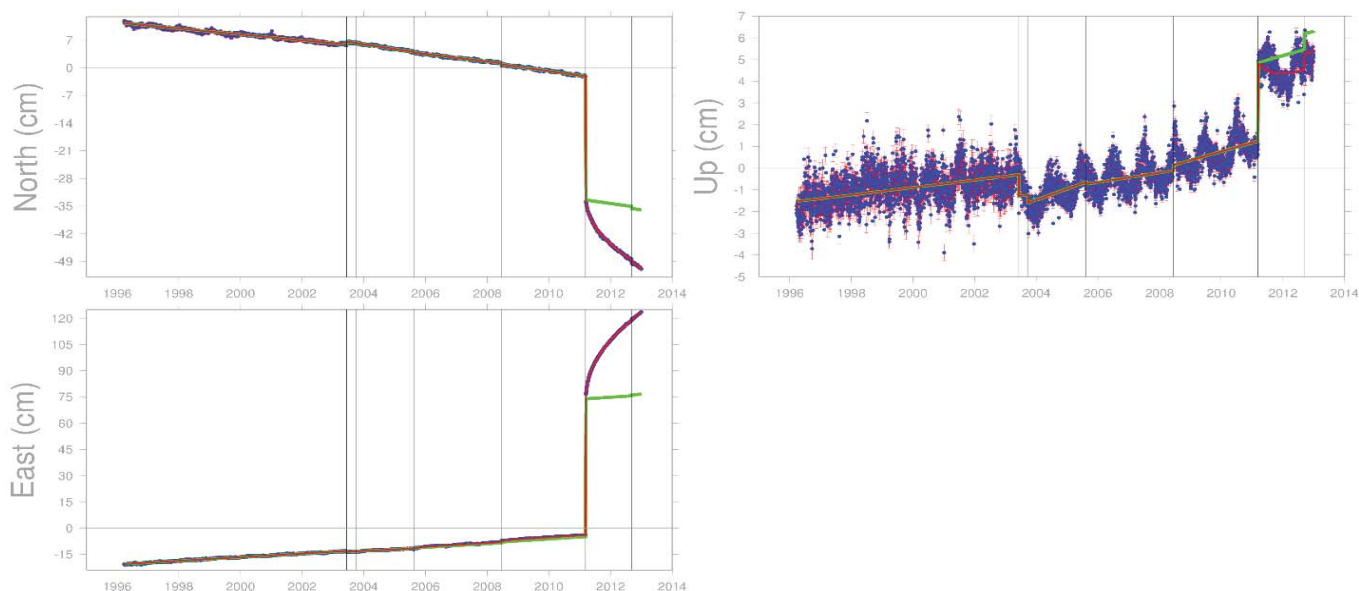
Наиболее частыми видами деформаций являются оползни, оседания и просадки, мульды сдвижения, землетрясения. Оползни возникают из-за смещений масс горных пород по склону под воздействием собственного веса. Мульды сдвижения поверхности – под влиянием выработки подземным способом.

Деформации земной поверхности, происходящие при землетрясениях, различаются по интенсивности, по пространственным и временным масштабам. По времени действия такие деформации подразделяются на косейсмические – происходят непосредственно в момент землетрясения, и постсейсмические – длящиеся многие годы после сейсмического события. Косейсмические деформации наблюдаются как сейсмологическими, так и геодезическими методами. Постсейсмические деформации наблюдаются только геодезическими методами или моделируются. В настоящее время данную деформацию с высокой точностью можно отслеживать в том числе и с применением ГНСС аппаратуры [9-16].

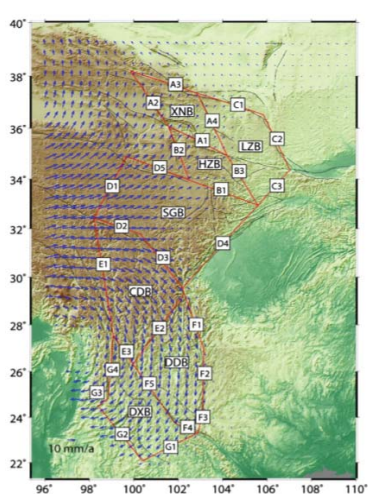
На рисунке 1 продемонстрирован резкий сдвиг в определенных координатах пункта методом ГНСС (синяя линия) в связи с землетрясением в Японии 2011 года [16].

Другим видом деформации земной поверхности является субдукция, которая представляет собой процесс продвижения литосферных плит друг под друга. Движение литосферных плит является одним из самых серьезных видов деформаций земной поверхности, так как может достигать значений от 5 мм до 9.5 см в год. Ряд стран специально развивают на своей территории региональные деформационные сети, такие как: Китайская Народная Республика (КНР) (260 и 2000 станций (СМОНОС)) [17-19] и Турция [20].

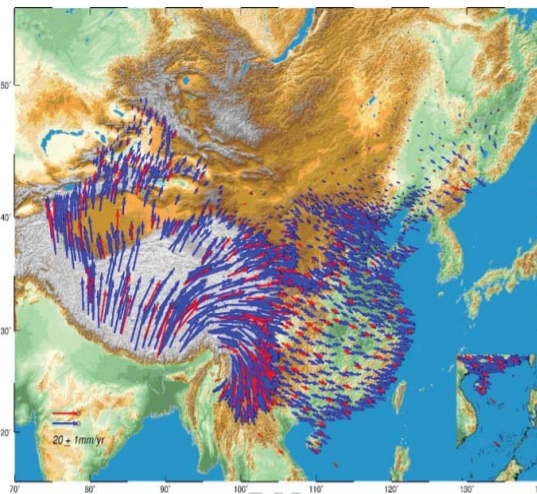
На рисунках 2 и 3 подремонтированы изменения координат точек земной поверхности, выполненные с применением ГНСС наблюдений на Тибетском плато и на всей территории КНР.



**Рис. 1.** Изменение координат пункта с кодом 0194 в Японии. График взят с официального сайта Международной Службы Вращения Земли (IERS-ITRF) [16]



**Рис. 2.** Деформации Тибетского плато



**Рис. 3.** Деформации литосферных плит на территории КНР

На основании приведенных данных, составлена сводная таблица, в которой указаны максимальные, средние и минимальные скорости различных деформационных процессов (таблица 2). Опираясь на отражённые в ней величины, можно сделать вывод, что максимальную скорость деформацией можно наблюдать с применением СГА. Для определения минимальной скорости нужны специальные и протестированные образцы аппаратуры, а также методики, позволяющие оценивать изменения пространственных координат на миллиметровом уровне.

Таблица 2

Скорости деформационных процессов

Тип деформации	Максимальная скорость	Средняя скорость	Минимальная скорость
1		3	4
Косейсмические деформации	5,3 м за 1 год	50 см за 1 год	4 см за 1 год
Постсейсмические деформации	41 см / год	5 см / год	0,2 см / год
Движение земной коры	9,5 см/год	5 см / год	0,4 см/год
Мульды сдвижения и оседания земной поверхности	39,1 см/год	10 см / год	1,5 см/год
Движение на разломах	20 см/год	5 см / год	1 мм / год
Карстовые деформации	56,8 см/год	-	0, см/год

Для определения требований к точности выполнения системой смещений фазового центра СГА рассмотрим результаты двух экспериментальных исследований:

- 1) исследование точности относительного кинематического позиционирования по измерениям на нулевой базе.
- 2) исследование точности позиционирования в режиме «кинематика в реальном времени» при разных расстояниях между подвижным и опорным приёмниками.

**Первое исследование** выполнено для определения средней квадратической погрешности (СКП) относительного кинематического позиционирования по сигналам GPS и ГЛОНАСС по измерениям на нулевой базе. Под «нулевой базой» имеется в виду подключение двух образцов СГА к одной антенне ГНСС при помощи делителя сигналов. В исследовании использованы два приёмника NovAtel FlexPak6 с одинаковыми характеристиками, одна ГНСС антенна NovAtel GNSS-750 и ноутбук с установленной программой Novatel Connect.

По результатам оценки точности для рассмотренного сеанса (общая длина сеанса 65000 секунд) получены следующие параметры:

- 1) Для измерений по сигналам GPS:  $m_X = 1.6$  мм,  $m_Y = 1.3$  мм,  $m_Z = 10.2$  мм;
- 2) Для измерений по сигналам ГЛОНАСС:  $m_X = 9.6$  мм,  $m_Y = 5.1$  мм,  $m_Z = 11.6$  мм;

Полученные значения СКП искажены имеющимися во временных рядах выбросами и не вполне корректно характеризуют точность полученных результатов позиционирования.

В качестве дополнительной характеристики точности вычислено значение погрешности, которое не будет превышено в 95 процентах эпох ( $M$ ).

- 1) Для измерений по сигналам GPS:  $M_X = 2$  мм,  $M_Y = 2$  мм,  $M_Z = 5$  мм;
- 2) Для измерений по сигналам ГЛОНАСС:  $M_X = 3$  мм,  $M_Y = 3$  мм,  $M_Z = 6$  мм;

В качестве опорных станции использовались четыре ДГС (условно обозначенные как: B1, B2, B3, B4) расположенные на расстояниях 32.7 км, 44.2 км, 52.1 км, 81.1 км соответственно. Исходя из паспортных технических характеристик СГА Уральского оптикомеханического завода (УОМЗ) МР-8 средние квадратические ошибки позиционирования в плане не должны превышать  $m_{P,B1} = 43.7$  мм,  $m_{P,B2} = 54.2$  мм,  $m_{P,B3} = 62.1$  мм,  $m_{P,B4} = 81.1$  мм. СКП по высоте не должны превышать  $m_{H,B1} = 53.7$  мм,  $m_{H,B2} = 64.2$  мм,  $m_{H,B3} = 72.1$  мм,  $m_{H,B4} = 91.1$  мм.

**Второе исследование** проведено для определения СКП позиционирования в режиме «кинематика в реальном времени» при разных расстояниях между подвижным и опорным приёмниками. Для проведения исследования в качестве подвижных приёмников два образца СГА УОМЗ МР-8. Используемые СГА позволяют производить кодовые измерения по сигналам GPS, ГЛОНАСС, Galileo, BDS с дискретностью до 10 Гц. Подвижные приёмники устанавливались на коротком базисе (длина базиса составляет 0.2 метра). Для каждой установки базовой станции (B1, B2, B3, B4) производился синхронный сеанс позиционирования режиме RTK на обоих подвижных приёмниках. Для передачи дифференциальных поправок между опорным и подвижными приёмниками использовался встроенный сотовый модем СГА УОМЗ МР-8. Для передачи данных применялся протокол NTRIP.

По результатам исследования получены временные ряды отклонений измеренной длины базиса от истины (рис. 4) и отклонений координат от среднего арифметического (рис. 5).

Полученные временные ряды использованы для оценки точности позиционирования и измерения длины базиса, результаты которой представлены в таблице 3.

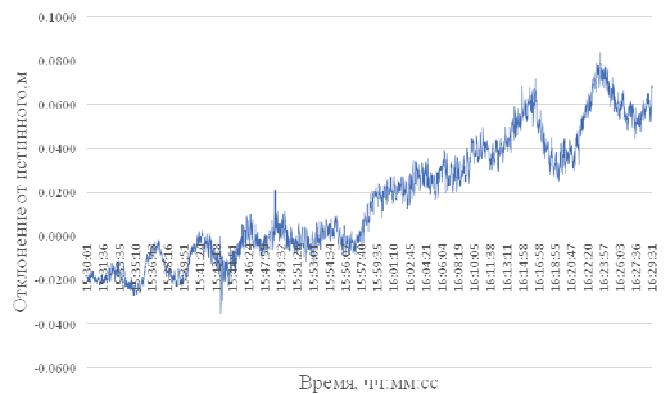


Рис. 4. Отклонения измеренной длины базиса от истины для четвертой установки базовой станции

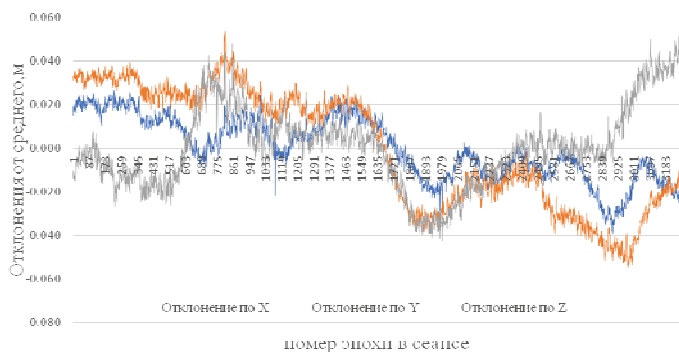


Рис. 5. Отклонения координат от среднего арифметического для четвертой установки базовой станции

Таблица 3

Оценка точности позиционирования в режиме «кинематика в реальном времени»

Сеанс	Ошибка по оси X, мм	Ошибка по оси Y, мм	Ошибка по оси Z, мм	Ошибка в плановом смещении, мм
1		7	14	6
2		6	13	
3	1	8	11	9
4		10	12	
5		7	12	4
6		7	12	
7	2	17	29	32
8	1	27	18	

Исходя из проведенного анализа, сформулированы следующие требования к проектируемой системе:

- 1) Дискретность смещений в плане и по высоте должна находиться на субмиллиметровом уровне;
- 2) Точность смещений в плане и по высоте должна находиться на субмиллиметровом уровне;
- 3) Система должна обеспечивать как линейные смещения в плане и по высоте, так и вращательные движения;
- 4) Система должна обеспечивать смещения в широких пределах, не менее 50 см в плане и 20 см по высоте;
- 5) Система должна обеспечивать скорость линейных смещений не менее 5 см в секунду;
- 6) Система должна обеспечивать поворот антенны СГА вокруг своей оси;
- 7) Система должна обеспечивать возможность одновременных смещений в плане и по высоте, а также вращательных движений;
- 8) Система должна обеспечивать возможность установки СГА, не оснащенных аккумуляторными батареями (обеспечивает возможность подключения внешнего питания к СГА, установленной на такой системе);
- 9) Система должна корректно функционировать при установке антенн ГНСС весом до трех килограмм;
- 10) Система должна обеспечивать автоматизированное выполнение заданной программы смещений.

### Конструкция системы

Общая схема собранной автоматизированной системы пространственных смещений фазового центра СГА представлена на рисунке 6.

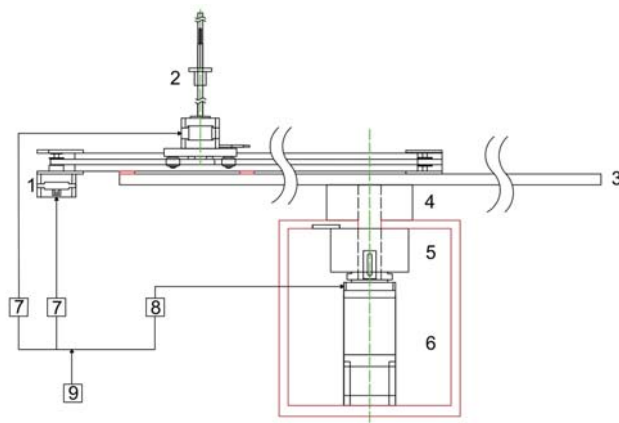


Рис. 6. Общая схема системы

Рассмотрим каждый закрепительный узел системы в отдельности. Узел 1 – объединение линейного шагового актуатора с кареткой линейного модуля L-500-4247 (рис. 7).

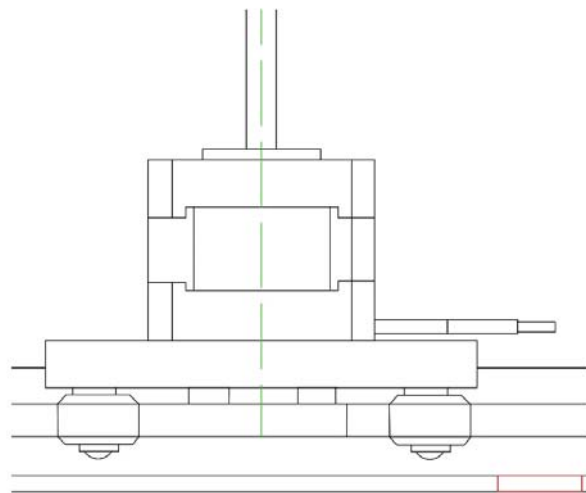


Рис. 7. Узел 1. Вид сбоку

Данное совмещение позволяет производить смещения в горизонтальной плоскости и параллельно с этим, изменять вертикальное положение закрепленной СГА. Ось актуатора проходит по центру каретки. Каретка имеет перфорированную структуру, что позволяет усилить надёжность крепления актуатора. Актуатор управляется контроллером шагового двигателя SMSD-1.5Modbus. На рисунке 8 представлен вид данного узла сверху и сбоку.

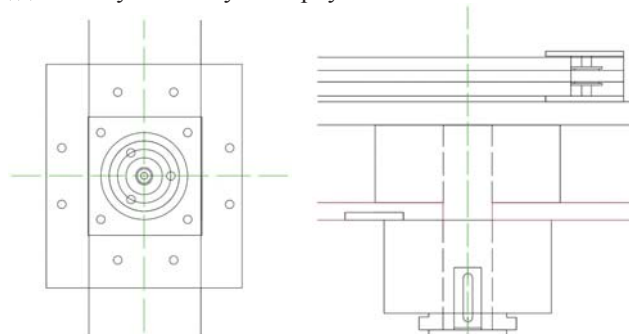


Рис. 8. Узел 2. Вид сверху и вид сбоку



Через центр алюминиевой плиты проходит ось вращения конструкции. Ось вращения совпадает с центром каретки при её максимальном смещении в сторону центральной части плиты (узел 2).

К нижней части подшипникового узла прикрепляются металлические плиты, которые образуют короб, контур которого отмечен красным цветом на рисунке 9 и 10. Внутри короба размещаются контактное кольцо со сквозным отверстием на вал H2586-0610 и шаговый двигатель с редуктором ШДР57-3.0-20-1/25 (узел 3), изменение шага которого придаёт системе вращательное движение. Шаговый двигатель с редуктором управляется программируемым блоком управления шаговыми двигателями SMSD-4.2LAN. На рисунке 10 продемонстрирован вид снизу. Каждая деталь отмечена своим цветом.

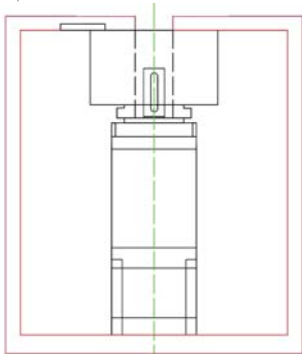


Рис. 9. Узел 3. Вид сбоку

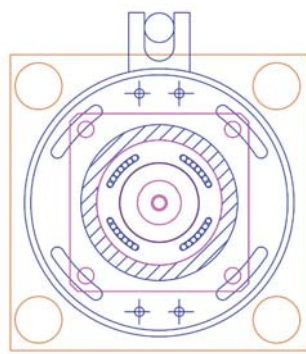


Рис. 10. Узел 3. Вид снизу

Узел 4 – Совмещение модуля линейного смещения и шагового двигателя FL42STH. Комплексирование модуля шаговым двигателем позволяет перемещать каретку в горизонтальной плоскости с заданным шагом. К шаговому двигателю подключен контроллер SMSD-1.5Modbus для управления смещениями.

На рисунке 12 показана электронная схема системы. Все электронные элементы подключены к сети питания, а именно Программируемый блок управления шаговыми двигателями SMSD-4.2LAN и два блока Контроллеров шагового двигателя SMSD-1.5Modbus. Электропитание осуществляется через источник питания LRS-350-24 MW.

Программируемые контроллеры шаговых двигателей SMSD-1.5Modbus и SMSD-4.2LAN предназначены для автоматизированного управления исполнительными механизмами с использованием шаговых двигателей на базе программно-технических комплексов.

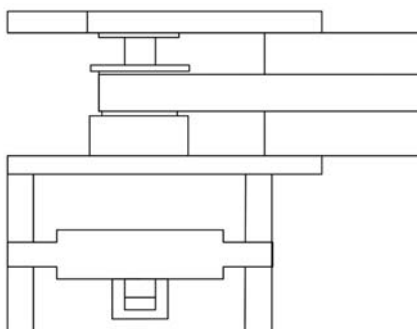


Рис. 11. Узел 4. Вид сбоку

От программируемого блока управления шаговыми двигателями SMSD-4.2LAN подпитывается и управляется линейный модуль L-500-4247 с верхним креплением двигателя.

От первого программируемого контроллера шаговых двигателей SMSD-1.5Modbus подпитывается и управляется Шаговый двигатель FL42STH47-1684A. Этот двигатель используется для передвигания по нормали вешки с установленным СГА по высоте (узел 1, как отображено на рис. 7).

От второго Программируемого контроллера шаговых двигателей SMSD-1.5Modbus подпитывается и управляется Шаговый двигатель с редуктором ШДР57-3.0-20-1/25. Этот двигатель необходим для обеспечения вращения всей конструкции относительно своей оси (узлы 2 и 3, как отображено на рис. 8-10).



Рис. 12. Схема электропитания и управления системой

Итоговые технические характеристики разработанной системы, которые представлены в таблице 4.

Таблица 4

Перечень полученных технических характеристик разработанной системы

Наименование	Значение
1	
Основные типы движений	Линейные перемещения в плане; Линейные перемещения по высоте; Движение по круговой траектории;
Количество размещаемых антенн СГА	1
<b>Линейные перемещения в плане</b>	
Число осей линейного смещения в плане	1 ось
Диапазон линейных смещений в плане	500 мм
Шаг линейных смещений в плане	0,2 мм
Номинальная скорость линейного перемещения	100 мм/с
Один полный оборот вала	40 мм
<b>Линейные перемещения по высоте</b>	
Диапазон линейных смещений по вертикали	230 мм
Шаг линейных смещений по вертикали	0,05 мм
<b>Движение по круговой траектории</b>	
Минимальный радиус	0 мм
Максимальный радиус	500 мм
Величина полного шага	1,8 град
Погрешность углового шага	± 0,09 град

## Выводы

На основе выполненного анализа, а также сформированных требований к системе был разработан проект автоматизированной системы пространственных смещений фазового центра СГА. Разработанная система позволяет производить одновременные смещения в плане и по высоте (путём комбинации плановых и линейных сдвигов), а также выполнять вращение вокруг оси с радиусом от 0 до 500 мм. Указанная реализация не требует постоянного закрепления и может быть оперативно перемещена. Диапазон линейных смещений системы в плане составляет 500 мм. Диапазон линейных смещений по вертикали составляет 230 мм. Шаг линейных смещений не превышает 0,2 мм в плане и 0,05 мм по высоте. Приведённые выше технические характеристики позволяют использовать разработанную систему для кинематических испытаний СГА и исследований в области кинематического позиционирования по сигналам ГНСС.

## Литература

- 1) *Фялковский А.Л.* Экспериментальная установка для исследования методов обработки данных, полученных с использованием ГНСС // Изв. вузов «Геодезия и аэрофотосъёмка». 2018. Т. 62. No 1. С. 27–34. doi: 10.30533/0536-101X-2018-62-1-27-34.
- 2) *Manzini, N., Orcesi, A., Thom, C., Brossault, M.-A., Botton, S., Ortiz, M., & Dumoulin, J.* Performance analysis of low-cost GNSS stations for structural health monitoring of civil engineering structures.. Structure and Infrastructure Engineering, (2020). 1–17. doi:10.1080/15732479.2020.1849
- 3) *Li W., Fan P., Cui X., Zhao S., Ma T., Lu M.* A Low-Cost INS-Integratable GNSS Ultra-Short Baseline Attitude Determination System. Sensors. 2018. 2114. 10.3390/s18072114.
- 4) *Biagi L., Grec Florin-Catalin, Negretti M.* Low-Cost GNSS Receivers for Local Monitoring: Experimental Simulation, and Analysis of Displacements. Sensors (Basel, Switzerland). 2016. 16. 10.3390/s16122140.
- 5) *Hamza V., Stopar B., Sterle O.* Testing the Performance of Multi-Frequency Low-Cost GNSS Receivers and Antennas. Sensors. 2021. 2029. 10.3390/s21062029.
- 6) *Бесимбаева О.Г., Уставич Г.А., Олейникова Е.А.* Мониторинг деформаций земной поверхности на подрабатываемых территориях // Интерэкспо Гео-Сибирь. 2019. №1. URL: <https://cyberleninka.ru/article/n/monitoring-deformatsiy-zemnoy-poverhnosti-na-podrabatyvaemyh-territoriyah> (дата обращения: 26.11.2020).
- 7) *Тимофеев В.Ю., Ардюков Д.Г., Тимофеев А.В., Бойко Е.В.* Современные движения земной поверхности Горного Алтая по GPS-наблюдениям // Геодинамика и тектонофизика. 2019. №1. URL: <https://cyberleninka.ru/article/n/sovremennyye-dvizheniya-zemnoy-poverhnosti-gornogo-altaya-po-gps-nablyudeniya> (дата обращения: 26.11.2020).
- 8) *Carlà T., Tofani V., Lombardi L., Raspini F., Bianchini S., Bertolo D., Thuegaz P., Casagli N.* Combination of GNSS, satellite InSAR, and GBInSAR remote sensing monitoring to improve the understanding of a large landslide in high alpine environment. Geomorphology. 2019. № 335. Pp. 62-75, ISSN 0169-555X
- 9) *Amiri M., Mousavi Z., Atzori S., et al.* Studying postseismic deformation of the 2010–2011 Rigan earthquake sequence in SW Iran using geodetic data, Tectonophysics. 2020. 10.1016/j.tecto.2020.228630
- 10) *Martens H., Simons M., Owen S., Rivera L.* Observations of Ocean Tidal Load Response in South America from Sub-daily GPS Positions. Geophysical Journal International. (2016). 205. ggw087. 10.1093/gji/ggw087.
- 11) *Шестаков Н.В., Сысоев Д.В., Герасименко М.Д., Титков Н.Н., Верхотуров А.Л., Газарский Н.А., Кишкина А.К., Годзе М., Такахаши Х.* Об определении малых «мгновенных» вертикальных смещений земной поверхности ГНСС-методами. Современные проблемы дистанционного зондирования Земли из космоса. 2019. т. 16. № 4. С. 33-44.
- 12) *Jiang Z., Yuan L., Huang D., Yang Z., Hassan, A.* Postseismic deformation associated with the 2015 Mw 7.8 Gorkha earthquake, Nepal: Investigating ongoing afterslip and constraining crustal rheology. Journal of Asian Earth Sciences.2018. № 156. Pp. 1-10. doi:10.1016/j.jseas.2017.12.039
- 13) *Castro-Perdomo N., Viltres R., Masson F., Klinger Y., Shaozhuo L., Maher D., Patrice U., Jean-Daniel B., Rémi M., A. Abdulaziz, Z. Hani, Reilinger R., Mai P., Sigurjón J.* Interseismic deformation in the Gulf of Aqaba from GPS measurements. Geophysical Journal International. 2021.228. 10.1093/gji/ggab353.
- 14) *Hamiel, Y., Masson, F., Piatibratova, O., Mizrahi, Y.* GPS measurements of crustal deformation across the southern Arava Valley section of the Dead Sea Fault and implications to regional seismic hazard assessment. Tectonophysics, 2018. 724-725, 171–178. doi:10.1016/j.tecto.2018.01.01
- 15) *He P., Wang Q., Ding K., Li J., Zou R.* Coseismic and postseismic slip ruptures for 2015 M w 6.4 Pishan earthquake constrained by static GPS solutions. Geodesy and Geodynamics. 2016. № 7(5). Pp. 323–328. doi:10.1016/j.geog.2016.07.004
- 16) *Ishitsuka, K., Matsuoka, T., Nishimura, T., Tsuji, T., & ElGharbawi, T.* (2017). Ground uplift related to permeability enhancement following the 2011 Tohoku earthquake in the Kanto Plain, Japan. Earth, Planets and Space, 69(1). doi:10.1186/s40623-017-0666-7
- 17) *Gunawan E., Widiyantoro S., Zulfakriza Meilano I., Pratama C.* Postseismic deformation following the 2 July 2013 M 6.1 Aceh, Indonesia, earthquake estimated using GPS data. Journal of Asian Earth Sciences. 2019. doi:10.1016/j.jseas.2019.03.020
- 18) *Yu J., Tan K., Zhang C., Zhao B., Wang D., Li Q.* Present-day crustal movement of the Chinese mainland based on Global Navigation Satellite System data from 1998 to 2018. Advances in Space Research. 2019. Volume 63. Issue 2. Pp 840-856, ISSN 0273-1177
- 19) *Hao M., Freymueller J. T., Wang Q., Cui D., Qin S.* Vertical crustal movement around the southeastern Tibetan Plateau constrained by GPS and GRACE data. Earth and Planetary Science Letters. 2016. Volume 437. Pp 1-8. ISSN 0012-821X
- 20) *Gurbuz G., Aktug B., Jin S., Hakan Kutoglu S.* A GNSS-Based Near Real Time Automatic Earth Crust and Atmosphere Monitoring Service for Turkey. Advances in Space Research. 2020. doi:10.1016/j.asr.2020.07.026



## DESIGN OF AN AUTOMATED SYSTEM OF SPATIAL DISPLACEMENTS OF THE PHASE CENTER OF SATELLITE GEODETIC EQUIPMENT

**DMITRY A. MOROZOV**

Moscow, Russia, dez.data@mail.ru

**DMITRY A. KUZNETSOV**

Moscow, Russia, dmitri-kuznetsov-94@mail.ru

**DMITRY E. LEVE**

Moscow, Russia, dmleve@yandex.ru

**ALEXEY Yu. PERMINOV**

Moscow, Russia, varhood@gmail.com

**KEYWORDS:** *automated system, GNSS, GNSS antenna phase center offset systems, satellite geodetic equipment.*

### ABSTRACT

**Introduction:** Usually special experimental installations are using for assessing the accuracy of determining the coordinates which obtained by various positioning methods and data processing technologies. Them also referred as systems of spatial displacements of the antenna phase center. In this paper decried the designing process of an automated system of spatial displacement of the satellite geodetic equipment phase center. **Purpose of work:** development of an automated system of spatial displacements of the phase center of satellite geodetic equipment. **Methods:** in this course of work, studies were carried out for aiming at potential requirements for an automated system of spatial displacements of the phase center. There're additional analysis of the design and purpose of existing systems as well as the development of a system. The results of this work was list of established requirements. **Results:** was presented the analysis of domestic and foreign experience in the development and use of such systems, their classification and the most successful technical solutions in that branch. The requirements have been developed for system technical characteristics based on the analysis of the tasks which potentially could be solved.

The element base and the design of the system was selected and developed in accordance with the specified technical characteristics. The rotation of the antenna of the Global Navigation Satellite Systems could be made in a circle with a radius of 0 to 500 mm. In this case, the radius can be dynamically changed with an accuracy of 0.2 mm. In addition, the system allows you to change the position of the antenna of the Global Navigation Satellite Systems in height within the range from 0 to 230 mm with an accuracy of 0.05 mm. The developed system does not require permanent fixing and can be moved to the required area of work. The results of the work should be used to assemble a prototype of an automated system of spatial displacements of the phase center of satellite geodetic equipment. **Practical significance:** The developed system can be used to conduct kinematic tests of satellite geodetic equipment and conduct a wide range of studies within the framework of modeling the movements of a reference satellite geodetic station under conditions of anthropogenic and natural influences. **Discussion:** Further development of the system may include the determination of its metrological characteristics using methods of near photogrammetry

### REFERENCES

1. Fialkovskii A.L. (2018). Experimental equipment for investigation of data processing methods for GNSS. *Proceedings of universities "Geodesy and aerial photography"*. 58 (1): 27-34. (In Rus). doi: 10.30533/0536-101X-2018-62-1-27-34.
2. Manzini, N., Orcesi, A., Thom, C., Brossault, M.-A., Botton, S., Ortiz, M., & Dumoulin, J. (2020). Performance analysis of low-cost GNSS stations for structural health monitoring of civil engineering structures. *Structure and Infrastructure Engineering*, 1-17. doi:10.1080/15732479.2020.1849
3. Li W., Fan P., Cui X., Zhao S., Ma T., Lu M. (2018). A Low-Cost INS-Integratable GNSS Ultra-Short Baseline Attitude Determination System. *Sensors*. 2114. 10.3390/s18072114.
4. Biagi L., Grec Florin-Catalin, Negretti M. (2016). Low-Cost GNSS Receivers for Local Monitoring: Experimental Simulation, and Analysis of Displacements. *Sensors* (Basel, Switzerland). 16. 10.3390/s16122140.
5. Hamza V., Stopar B., Sterle O. (2021). Testing the Performance of Multi-Frequency Low-Cost GNSS Receivers and Antennas. *Sensors*. 2029. 10.3390/s21062029.
6. Besimbaeva O.G., Ustavich G.A., Oleinikova E.A. (2019). Monitoring of deformations of the earth's surface in undermined areas. *Interexpo Geo-Siberia*. No. 1. (In Rus)

7. Timofeev V.Y., Ardyukov D.G., Timofeev A.V., Boyko E.V. (2019). Modern movements of the Earth's surface in Gorny Altai based on GPS observations. *Geodynamics and Tectonophysics*. No. 1. (In Rus)
8. Carlo T., Tofani V., Lombardi L., Raspini F., Bianchini S., Bertolo D., Thuegaz P., Casagli N. (2019). Combination of GNSS, satellite InSAR, and GBInSAR remote sensing monitoring to improve the understanding of a large landslide in high alpine environment. *Geomorphology*. No. 335. Pp. 62-75, ISSN 0169-555X
9. Amiri M., Mousavi Z., Atzori S., et al. (2020). Studying postseismic deformation of the 2010-2011 Rigan earthquake sequence in SW Iran using geodetic data, *Tectonophysics*. doi: 10.1016/j.tecto.2020.228630
10. Martens H., Simons M., Owen S., Rivera L. (2016). Observations of Ocean Tidal Load Response in South America from Sub-daily GPS Positions. *Geophysical Journal International*. 205. ggw087. 10.1093/gji/ggw087.
11. Shestakov N. V., Sysoev D. V., Gerasimenko M. D., Titkov N. N., Verkhoturov A. L., Gagarsky N. A., Kishkina A. K., Godze M., Takahashi H. (2019). On the determination of small "instantaneous" vertical displacements of the earth's surface by GNSS methods. *Modern problems of remote sensing of the Earth from space*. Vol. 16.No. 4. P. 33-44 (In Rus)
12. Jiang Z., Yuan L., Huang D., Yang Z., Hassan, A. (2018). Postseismic deformation associated with the 2015 Mw 7.8 Gorkha earthquake, Nepal: Investigating ongoing afterslip and constraining crustal rheology. *Journal of Asian Earth Sciences*. No. 156. Pp. 1-10. doi:10.1016/j.jseaes.2017.12.039
13. Castro-Perdomo N., Viltres R., Masson F., Klinger Y., Shaozhuo L., Maher D., Patrice U., Jean-Daniel B., Remi M., A. Abdulaziz, Z. Hani, Reilinger R., Mai P., Sigurjen J. (2021). Interseismic deformation in the Gulf of Aqaba from GPS measurements. *Geophysical Journal International*. 228. 10.1093/gji/ggab353.
14. Hamiel, Y., Masson, F., Piatibratova, O., Mizrahi, Y. (2018). GPS measurements of crustal deformation across the southern Arava Valley section of the Dead Sea Fault and implications to regional seismic hazard assessment. *Tectonophysics*, 724-725, 171-178. doi:10.1016/j.tecto.2018.01.01
15. He P., Wang Q., Ding K., Li J., Zou R. (2016). Coseismic and postseismic slip ruptures for 2015 M w 6.4 Pishan earthquake constrained by static GPS solutions. *Geodesy and Geodynamics*. No. 7(5). Pp. 323-328. doi:10.1016/j.geog.2016.07.004
16. Ishitsuka, K., Matsuoka, T., Nishimura, T., Tsuji, T., & ElGharbawi, T. (2017). Ground uplift related to permeability enhancement following the 2011 Tohoku earthquake in the Kanto Plain, Japan. *Earth, Planets and Space*, 69(1). doi:10.1186/s40623-017-0666-7
17. Gunawan E., Widiyantoro S., Zulfakriza Meilano I., Pratama C. (2019). Postseismic deformation following the 2 July 2013 M 6.1 Aceh, Indonesia, earthquake estimated using GPS data. *Journal of Asian Earth Sciences*. doi:10.1016/j.jseaes.2019.03.020
18. Yu J., Tan K., Zhang C., Zhao B., Wang D., Li Q. (2019). Present-day crustal movement of the Chinese mainland based on Global Navigation Satellite System data from 1998 to 2018. *Advances in Space Research*. Vol. 63. Issue 2. Pp 840-856, ISSN 0273-1177
19. Hao M., Freymueller J. T., Wang Q., Cui D., Qin S. (2016). Vertical crustal movement around the southeastern Tibetan Plateau constrained by GPS and GRACE data. *Earth and Planetary Science Letters*. Vol. 437. Pp 1-8. ISSN 0012-821X
20. Gurbuz G., Aktug B., Jin S., Hakan Kutoglu S. (2020). A GNSS-Based Near Real Time Automatic Earth Crust and Atmosphere Monitoring Service for Turkey. *Advances in Space Research*. 2020. doi:10.1016/j.asr.2020.07.026

#### INFORMATION ABOUT AUTHORS:

**Dmitry A. Morozov** - Lecturer, Department of Applied Geodesy, Moscow State University of Geodesy and Cartography, Moscow, Russia, dez.data@mail.ru

**Dmitry A. Kuznetsov** - Lecturer, Department of Applied Geodesy, Moscow State University of Geodesy and Cartography, Moscow, Russia, dmitri-kuznetsov-94@mail.ru

**Dmitry E. Leve** - Lecturer of the Department of Applied Geodesy, Moscow State University of Geodesy and Cartography, Moscow, Russia, dmleve@yandex.ru

**Alexey Yu. Perminov** - Lecturer, Department of Applied Geodesy, Moscow State University of Geodesy and Cartography, Moscow, Russia, varhood@gmail.com

---

**For citation:** Morozov D.A., Kuznetsov D.A., Leve D.E., Perminov A. Yu. Design of an automated system of spatial displacements of the phase center of satellite geodetic equipment // H&ES Reserch. 2021. Vol. 13. No. No 5. P. 4-12. doi: 10.36724/2409-5419-2021-13-5-4-12 (In Rus)





doi: 10.36724/2409-5419-2021-13-5-13-28

# МЕТОДИКА ПРЕВЕНТИВНОЙ ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ОБЪЕКТОВ МОНИТОРИНГА НА ОСНОВЕ СИМВОЛЬНОГО ПРЕДСТАВЛЕНИЯ ВРЕМЕННЫХ РЯДОВ ИХ МЕТРИК

АЛЛАКИН

Владимир Васильевич<sup>1</sup>

## АННОТАЦИЯ

**Введение:** на основе анализа методов оценки временных рядов наблюдаемых параметров устройств информационно-телекоммуникационных сетей общего пользования разработать методику превентивной идентификации состояния объектов мониторинга, используя символическое представление временных рядов их метрик. **Цель исследования:** определить обобщенные универсальные характеристики временного ряда, по которым возможно оценить разнообразие наблюдаемых значений метрик, относящихся к определенной области состояния объекта мониторинга (классу его технического состояния). **Результаты:** превентивная идентификация аномального состояния сетевого элемента осуществляется путем выявления "запрещенных" кодовых слогов на кодовом слове, описывающем наблюдаемый временной ряд метрики. Данный подход к обработке временных рядов заимствован из символической динамики, применяемый в биоинформатике при анализе сложных нуклеотидных геномных последовательностей. В качестве обобщенной универсальной характеристики временного ряда использована энтропия кодовых слов, описывающая временной ряд, закодированный методом символического представления данных наблюдаемых метрик. Разработан алгоритм методики превентивной идентификации аномальной ситуации на временном ряду его параметров, состоящий из четырех этапов: на первом этапе осуществляется символическое кодирование временного ряда по возможным значениям параметров; на втором – производится оценка энтропии кодового слова, описывающего временной ряд наблюдаемой метрики; на третьем – обучается классификатор состояний объекта измерения на основе энтропии сдвигов; на четвертом – классифицируется состояние по тестовой выборке измерений, в которых измеряемая характеристика описывается своим законом распределения вероятностей сдвигов. **Практическая значимость:** при обнаружении аномального функционального состояния сетевого элемента осуществляется переход к особому режиму мониторинга, когда скважность опроса сервером мониторинга сетевого элемента значительно увеличивается с целью своевременного принятия превентивных управляющих воздействий на сетевую инфраструктуру и недопущения пропуска отказа (наступления аварии). **Обсуждение:** методика позволит в последующем сформировать порядок работы сервера мониторинга для идентификации функционального состояния сетевого элемента и информационно-телекоммуникационной сети общего пользования в целом.

## Сведения об авторе:

<sup>1</sup> аспирант, Федеральное государственное бюджетное образовательное учреждение высшего образования "Государственный университет морского и речного флота имени адмирала С.О. Макарова".  
г. Санкт-Петербург, Россия,  
vladimir@duduh.ru

**КЛЮЧЕВЫЕ СЛОВА:** сервер мониторинга, идентификация технического состояния, особый режим мониторинга, временные ряды, превентивная идентификация.

**Для цитирования:** Аллакин В.В. Методика превентивной идентификации состояния объектов мониторинга на основе символического представления временных рядов их метрик // Научно-технические исследования в космических исследованиях Земли. 2021. Т. 13. № 5. С. 13-28. doi: 10.36724/2409-5419-2021-13-5-13-28

## Введение

Изменение большого числа контролируемых характеристик информационно-телекоммуникационных сетей (ИТКС) общего пользования (ФЗ № 126 «О связи», 2003) и ее основных элементов (серверов, узлов коммутации, периферийных устройств, каналов передачи данных) носит характер случайного процесса [1, 2], представляемого временными рядами. При этом статистический характер принятия решений о функциональном состоянии сетевого элемента и ИТКС в целом особенно хорошо прослеживается с ростом размерности объекта и увеличением скважности его опроса серверами мониторинга, что существенно влияет на увеличение количества обрабатываемой измерительной информации (ИИ). А учитывая тот факт, что наблюдение за сетевыми объектами мониторинга осуществляется практически на протяжении всего их жизненного цикла, то задачи обработки временных рядов в современных подсистемах мониторинга справедливо относят к задачам анализа больших данных (*Big Data*) [2, 3].

Временной ряд случайного потока отказов, влияющего на показатели надёжных характеристик сетевых устройств ИТКС, можно представить случайным процессом [4], в основе которого всегда лежит математическая модель. При этом большинство моделей предполагают, что прогнозирование случайного процесса общего вида основано как на аддитивном представлении случайного процесса в виде суммы декомпозиций трендовой, периодической (циклической) и стохастической компонент, рис. 1, так и на мультипликативном их представлении, т. е. произведении данных компонент:

тренд случайного процесса (рис. 1, *a*) – некоторая детерминированная компонента, не содержащая периодических составляющих, кроме, тех, периоды которых заведомо больше интервала временного окна наблюдения случайного процесса;

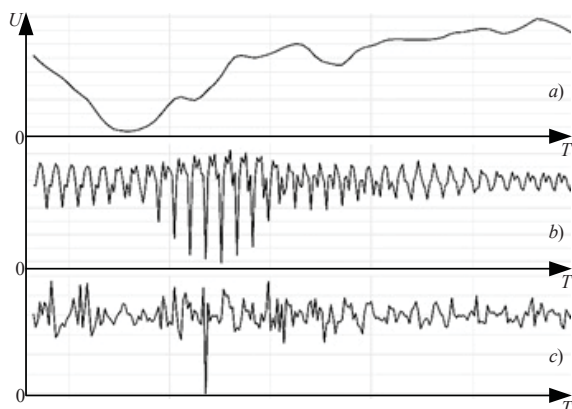


Рис. 1. Основные разновидности случайных процессов, представляемые временными рядами

периодическая (циклическая) компонента (рис. 1, *b*) – определяется как совокупность неслучайных гармонических колебаний, периоды которых заведомо меньше, чем интервал временного окна наблюдения случайного процесса;

случайная компонента (рис. 1, *c*) – центрированный случайный процесс.

В современных системах мониторинга ИТКС общего пользования (ОП) динамика объекта мониторинга (сетевого устройства, канала, сети) представляется как последовательность переходов между их стационарными состояниями. Примеры можно увидеть в ГОСТ 27.002-2015 по надежности, в соответствии с которым к основным видам состояния технических устройств (с точки зрения их надежности) относят: исправное, неисправное, работоспособное, предотказное, неработоспособное и предельное состояния. Это не противоречит рекомендациям Международного союза электросвязи (Rec. ITU-T M.3703), где вводятся следующие виды состояний: «неопределенное» (*Undefined, U*); «норма» (*Normal, N*); «незначительное нарушение» (*Minor, I*); «значительное нарушение» (*Major, J*); «критическое» (*Critical, C*); «авария» (*Fault, F*).

В связи с этим, основная задача системы мониторинга состоит в оперативном событийном уведомлении лица принимающего решение (ЛПР) о смене состояния сети ИТКС ОП или ее сетевых элементов. Как правило, в конечной интерпретации ЛПР, таких основных состояний всего два «норма» – сетевой элемент выполняет свои функции и «авария» – сетевой элемент не может выполнять свои функции. Остальные состояния служат для уведомления ЛПР о направлении динамики процесса – от «нормы» к «аварии» и от «аварии» к «норме».

Рассматривая поведенческий подход [5] к мониторингу ИТКС ОП, необходимо отметить, что независимо от отечественной или международной классификации видов состояний технических устройств, в итоге, их интерпретация сводится к двум основным: «норма» и «авария». Динамика переходных процессов от «нормы» (*N*) к «аварии» (*F*) редко характеризуется явной последовательностью событий  $N - I - J - C - F$  через «незначительное нарушение» (*I*), «значительное нарушение» (*J*) и «критическое» (*C*). Обычно, в журнале регистрации событий наблюдается переходные процессы с колебаниями, при которых вполне возможен как временный возврат на менее критическое состояние, так и резкие скачки «через» состояние, или через несколько состояний (например:  $N - I - J - C - F$ ,  $N - J - C - F$ ,  $N - C - F$ , или даже  $N - F$ ), которые не были идентифицированы по причине малой скважности опроса сетевого элемента сервером мониторинга.

Решение вопроса периодичности опроса объектов мониторинга подсистемой контроля является самостоятельной оптимизационной задачей, но, в то же время, полученное ее решение не будет универсальным на множестве контролируемых метрик для разнородных сетевых элементов различных ИТКС. Каждый производитель старается решить данную задачу для своего оборудования самостоятельно. Так, для временных рядов, характеризующихся трендом случайного процесса (рис. 1 *a*), наиболее используемым в подсистемах мониторинга, является триггерный механизм идентификации технического состояния (например, активно используемый в *Cisco*) и позволяющий устранить дублирование событий в журнале в случае колебаний измеримой характеристики вблизи порога (т. н. эффект «дребезга нуля»). Метод заключается в назначении пары пороговых значений «возрастающего» и «убывающего» порогов. Событие генерируется, когда превышает «возрастающий» порог. Как только этот порог пре-

вышен, событие не генерируется снова, пока не будет пересечен «убывающий» порог. Наглядно метод гистерезиса показан на рис. 2.

Поскольку начальное состояние было настроено на срабатывание при повышении «возрастающего» порога, в точке *A* сигнал тревоги не генерируется. По мере того, как значение измерения увеличивается до уровня выше «возрастающего» порога, сигнал тревоги генерируется в точке *D*. Никаких сигналов в точках *E*, *F*, *G*, *H* или *I* не генерируется до тех пор, пока не будет сгенерирован сигнал о пересечении «убывающего» порога (точка *J*). И снова в точке *K* не будет генерироваться никаких дополнительных сигналов тревоги, пока не произойдет пересечение «возрастающего» порога в точке *L*. В итоге, без гистерезиса было бы сгенерировано 12 аварийных сигналов, с гистерезисом генерируются только три. Зачатую, сокращение генерации аварийных сигналов бывает более значительным. Однако данный механизм гистерезиса не приводит к надежной идентификации направленной динамики процесса. Нужен поиск новых подходов к решению такого класса задач.



Рис. 2. Применение триггерного механизма для сокращения числа событий вследствие эффекта «дребезга нуля»

Рассмотрим временной ряд с использованием символического представления, описанного в [6] и применяемого в разделе символической динамики из теории динамических систем, когда для описания последовательностей измерений состояния системы пользуются символами некоторого заданного алфавита. Такой подход наиболее эффективен в описании и исследовании детерминированных систем, в которых из-за ограниченной возможности измерения возникает сходство со случайным процессом. При этом описание временного ряда и динамики его изменения возможно в терминах топологических аналогов марковских процессов, т. е. с помощью матриц возможных переходов между классами технического состояния (ТС) системы. Непосредственно для такого описания необходимо задать алфавит, который бы наиболее подходил для представления разбиения пространства ее состояний на области, которые бы соответствовали измеряемым значениям параметров (метрик). Данная оценка была заимствована теорией символической динамики из биоинформатики, где активно используется для оценки сложности нуклеотидных геномных последовательностей [7], например, очень длинных последовательностей ДНК [8]. Причем вполне естественно оценивать сложную бесконечную допустимую последовательность числом различных

конечных слов, входящих в нее. Тогда задача определения вторичной структуры временного ряда (структуры локальных конфигураций) [9] формулируется как задача преобразования слов в алфавите метрик в слова над алфавитом локальных конфигураций, используя метод скользящего окна (кодов определенных слогов в кодовых словах) [10]. При этом количественная оценка временного ряда производится с помощью топологической энтропии или метрической энтропии по Колмогорову.

**Постановка задачи.** При заданном алфавите  $\Sigma$  классов технических состояний (*A* – исправное, *B* – неисправное, *C* – работоспособное, *D* – предотказное, *E* – неработоспособное, *F* – предельное) сетевого элемента, рассмотрим временной ряд его метрики произвольной природы  $T = \{(f_i, t_i), i = 1, n\}$ , где  $f_i$  – значение характеристики наблюдаемого процесса (изменение метрики параметра сетевого устройства) в момент времени  $t_i$ ,  $n$  – число наблюдений (временных отсчетов).

**Необходимо** определить обобщенные универсальные характеристики данного временного ряда, по которым возможно оценить разнообразие наблюдаемых значений параметров (метрик), относящихся к определенной области состояния объекта мониторинга (классу его технического состояния).

Для решения задачи *на первом этапе* осуществляем символическое кодирование временного ряда по возможным значениям параметров; *на втором* – производим оценку энтропии кодового слова, описывающего временной ряд наблюдаемой метрики; *на третьем* – обучаем классификатор состояний объекта измерения на основе энтропии сдвигов; *на четвертом* – классифицируем состояния по тестовой выборке измерений, в которых измеряемая характеристика описывается своим законом распределения вероятностей сдвигов.

### Анализ временного ряда по значениям метрик

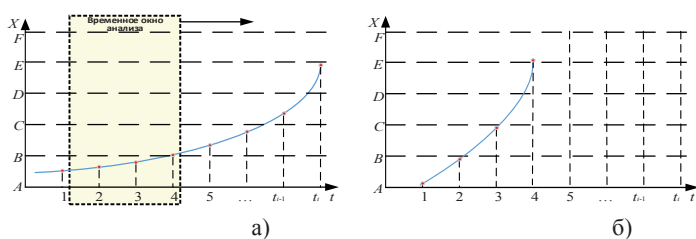
Необходимость универсализации разнородных временных рядов в пространстве их кластеризации налагает требования к их обобщенным универсальным характеристикам, определенные значения которых интерпретируются координатами точки, которая представляет рассматриваемый временной ряд в таком пространстве. В то же время сложности универсализации связаны с тем, что различные временные ряды имеют разную точность измерений, т. е. число значащих цифр в значении характеристики наблюдаемого процесса  $f_i$ , а также вариацию этих значений на различных интервалах времени  $t_i$ , что видно из рис. 3.

Для универсализации временных рядов в [6] предлагается масштабирование значений наблюдаемой функции  $f_i$ , а также построение исходя из этого строки символов, которые отражали бы динамику их числовых значений. Для этого определяется размах варьирования значений рассматриваемого временного ряда:  $V = y_{\max} - y_{\min}$ , где  $y_{\min} = \min_{i=1,n} f_i$ ,  $y_{\max} = \max_{i=1,n} f_i$ , на котором вводится разбиение  $y_i$ ,  $i = 1, m$  диапазона  $[y_1, y_m]$ , причём  $y_1 = y_{\min}$ ,  $y_m = y_{\max}$ .

Однако, поскольку значения  $f_i$  временного ряда могут попадать и на границу разбиений, то правильно рассматривать диапазон  $[y_i, y_{i+1}) = \{y \mid y_i \leq y < y_{i+1}, i = 1, m-1\}$ .



В данном случае определение числа разбиений  $k$  ( $k = m - 1$ ) всего диапазона наблюдения значений параметра (метрики) на сегменты, а также определение их внутренних границ является самостоятельной оптимизационной задачей [10] с применением бикритериального метода построения гистограмм, которая уже была решена в [11]. Число разбиений  $k$  диапазона наблюдения параметра, полученных данным методом и определяет мощность алфавита описания.



**Рис. 3.** Символьное представление временного ряда наблюдаемого параметра: а) с медленным; б) лавинообразным нарастанием аварийной ситуации (отказа)

Например, на рис. 3 приведено разбиение размаха временного ряда на символы  $A, B, C, D, E, F$  выбранного алфавита  $\Sigma$  (здесь символы алфавита  $\Sigma$  соответствуют прописным символам латинского алфавита). При этом последний элемент разбиения (на рис. 3 обозначен как «F»), очевидно также будет являться сегментом. Данными символами обозначаются разбиения значений наблюдаемой величины в порядке их возрастания. Так символ «A» – имя разбиения наименьших значений (по видам состояния соответствует исправному ТС сетевого элемента, когда все параметры имеют номинальные значения), а «E» – соответствующее аварии (отказу), «F» – предельному, когда дальнейшая эксплуатация опасна или нецелесообразна. Если измерения параметра (метрики) ведется в дискретное время, то описание значений временного ряда символами разбиений есть слово над алфавитом  $\Sigma$  в строке. Прохождением по временному ряду получается кодирование (представление) его строкой символов. Причем числовое значение  $f_i$  кодируется символом разбиения (сегмента), в котором оно находится: для рис. 3 а) – {AABBBCD...}; для рис. 3 б) – {ABE...}. Если наблюдаемый процесс описывается резким увеличением значений параметра (наблюдаемой величины), равно как и резким спадом за один временной интервал относительно нормального тренда его изменения (последовательного перехода из одного разбиения (сегмента) в другой), то получаемые кодовые слова, характеризующие временной ряд не будут содержать некоторых слогов. Так, кодовое слово временного ряда показанного на рис. 3 б) не содержит слога «CD». Данная ситуация идентифицируется как лавинообразный процесс развития аварии (отказа).

Такой подход позволяет осуществить интервальный анализ временного ряда, где в качестве интервала может рассматриваться «скользящее окно», последовательно сдвигающееся вдоль временного ряда и отслеживающее появление аномальных предаварийных ситуаций, или отказов, путем сравнения просматриваемых в «скользящем окне» слогов в наблюдаемом кодовом слове-строке временного ряда с «запрещенными» кодовыми слогами, идентифицирующими аномальное состояние.

При этом временной ряд, имеющий  $n$  временных отсчетов (наблюдений), будет представлен в виде кодового слова-строки из  $n$  символов над алфавитом  $\Sigma$ , а ширину «скользящего окна» можно подобрать оптимальным образом (для конкретной метрики индивидуально), учитывая физические процессы развития аномальных ситуаций и отказов в различных сетевых элементах, при различных режимах и условиях функционирования. Так, на рисунке 3 а) ширина скользящего окна анализа равна  $m = 3$ . Поскольку процессу возникновения отказа сетевого элемента, как правило, предшествуют во времени изменения значений параметров (метрик) с трендом выхода их за пределы эксплуатационных и профилактических допусков [12], то в ходе производственных испытаний и опытной эксплуатации технических устройств нарабатывается база «запрещенных» слогов кодовых слов, используемая в пространстве сдвигов «скользящего окна» путем сравнения с наблюдаемым результатом. Таким образом, выявление «запрещенных» слогов в кодовом слове-строке временного ряда может лечь в основу метода прогнозирования наступления аварии или отказа.

Для решения задачи масштабирования в [9] предложен диапазон значений временного ряда, который может быть как с равномерным разбиением, так и с вычислением длины и числа разбиений на основе аппарата математической статистики (при решении задач мониторинга – аппарата теории надежности). Для временных рядов конкретных контролируемых параметров данный вопрос индивидуален и зависит не только от номинальных величин параметра, но также от эксплуатационных и профилактических допусков на них [12]. Число разбиений при оценке функциональной надежности сетевых элементов, как правило, соответствует видам их ТС.

Как было отмечено выше, с точки зрения функциональной надежности эксплуатанта в большей степени интересует переход из работоспособного в неработоспособное («Авария» или «Отказ») состояние через промежуточное – предотказное ТС. Учитывая это, разбиение, соответствующее предотказному ТС может уточняться для каждого сетевого элемента или его измеряемого параметра. Очевидно, что различные временные ряды могут содержать не равные количества наблюдаемых значений. В рассматриваемом подходе символического кодирования это означает, что описание временного ряда будет представлено словами-строками различной длины в заданном фиксированном алфавите. В связи с чем, в [10] осуществлен переход от оценки абсолютной сложности строки по Колмогорову (от длины сжатой строки) к ее относительной оценке через коэффициент сжатия [13, 14].

### Анализ временного ряда по тенденциям изменения метрик

В ряде случаев для подсистемы мониторинга функциональной безопасности (надежности) интерес представляет не реальное изменение временного ряда в следующий дискрет времени, а изменение его тенденции. Сама по себе задача определения рациональных порогов идентификации в изменении тенденций достаточно сложна, поскольку необходимо определиться с критерием положительной тенденции или ее отсутствием (0,5 %, 1 %, 2 %...?).

При этом необходима либо специальная предварительная обработка исходных данных временных рядов, либо примене-



ние метода экспертных оценок, что, во втором случае носит субъективный характер и не является математически обоснованным. Само по себе использование метода символического кодирования значений временного ряда уже можно интерпретировать как предварительную обработку, а поскольку используемый в [9] бикритериальный метод построения разбиений гарантирует, что доверительный интервал для выборочного среднего в каждом разбиении будет не шире самого разбиения, то локализация значений, кодируемых одним символом алфавита  $\Sigma$ , является статистически достоверной. Из чего можно заключить, что, используя метод символического кодирования, изменение символа заданного для временного ряда алфавита  $\Sigma$  в следующий временной интервал и есть квалификация тенденции, в то время как изменение значения параметра, не выводящее его за полосу ширины разбиения – отсутствие какой-либо тенденции.

Продemonстрируем символическое описание временного ряда изменения значений параметра по тенденциям (рис. 4).

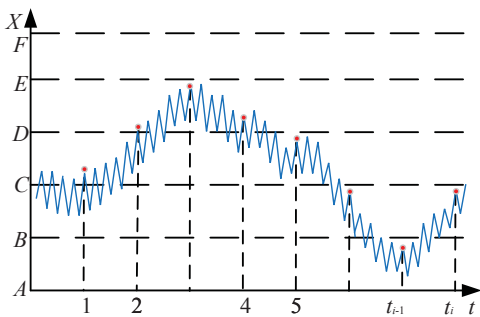


Рис. 4. Символьное описание временного ряда по тенденции изменения значения метрики

Для кодирования *по тенденциям* представленного на данном рисунке временного ряда используем алфавит  $\Sigma_{\text{тенд}} = \{-, 0, +\}$ , в котором символом «0» обозначено отсутствие тенденции в значении последующего временного интервала. Тогда при кодировании временного ряда в ранее определенном алфавите  $\Sigma_{\text{знач}} = \{A, B, C, D, E\}$  (по значениям) кодовое слово будет иметь вид:  $\{CDDDCBAB\}$ , а при кодировании того же временного ряда по тенденциям с использованием алфавита  $\Sigma_{\text{тенд}}$  кодовое слово будет выглядеть  $\{0+00---+\}$ , предполагая, что первый символ кода тенденции всегда имеет значение «0» (отсутствие тенденции).

С точки зрения теории надежности для подсистемы мониторинга важно, чтобы значения наблюдаемых параметров сетевых элементов находились при определенных режимах функционирования в стабильном состоянии (отсутствие тенденций). Для динамических систем с постоянно изменяющимися режимами работы (недогруженный, перегруженный и пр.) и изменением обрабатываемой нагрузки в символах кодовых слов, описывающие временные ряды наблюдаемых параметров всегда будут присутствовать тенденции. Для выявления разрушительных тенденций, вызывающих переход сетевого элемента из работоспособного состояния в состояние отказа (аварийное состояние) необходимо определить запрещенные полуслова (слоги) в описываемом временной ряд слове-строке. Как правило, аварий-

ному режиму функционирования предшествует некоторый временной интервал, соответствующий предотказному состоянию, характеризуемый повышенным риском возникновения отказа.

Предотказное состояние может быть связано с воздействиями на сетевой элемент многих внешних (ошибки персонала, условия эксплуатации, воздействия естественного и искусственного характера и пр.) и внутренних (производственные дефекты, программные сбои, перегруженные режимы работы и пр.) факторов. При этом задачей подсистемы мониторинга является своевременное обнаружение предотказного состояния сетевого устройства с целью оперативного (превентивного) принятия мер для недопущения развития отказа (аварии). С этих позиций применение метода символического кодирования как по значениям временных рядов, так и по тенденциям, позволяет заблаговременно обнаружить «запрещенную» комбинацию полуслов (слов) в кодовом слове, описывающем временной ряд значений контролируемых параметров. Тогда обнаружение развития отказа возможно по выявлению в кодовом слове временного ряда слогов, идентифицирующих стремительно развивающуюся тенденцию в сторону разбиения, характеризующую аварийной состояние объекта контроля (ОК) (для рассматриваемого примера рис. 3 и 4 – разбиение «E»). Так, при символическом кодировании значений временного ряда на рис. 3 a) факт перехода из режима нормального функционирования (символ разбиения – «A») к предотказному состоянию (символ разбиения «D») интерпретируется слогом «BCD» в слове-строке  $\{AAABBBBCD\dots\}$ , а на рис. 3 b) переход к отказу – слогом «ABE» в слове  $\{AABE\}$ .

При кодировании временного ряда по тенденциям аномальное состояние (поведение) системы (сетевого устройства) может идентифицироваться слогами типа  $\{++\}$ ,  $\{+++ \}$ , или  $\{-\}$ ,  $\{--- \}$ .

Соответственно подсистема мониторинга должна в ходе обработки кодового слова временного ряда выявлять подобные «запрещенные» комбинации слогов, характеризующие наступление предотказного состояния или отказа системы. Факт перехода объекта мониторинга в критическое состояние должен выявляться заранее для принятия превентивного управляющего воздействия. Такой реакцией подсистемы мониторинга на наступление предотказного ТС может быть управляющее воздействие на сеть (сетевой элемент) или перевода системы мониторинга в особый режим мониторинга.

В работе предлагается в качестве особого режима мониторинга использовать *увеличение скважности опросов* сервером мониторинга сетевого элемента по значениям наблюдаемых метрик, когда при выявлении наступления его предотказного состояния по агрегированной предварительно собранной статистике о сетевом устройстве для недопущения развития аварийной ситуации частота опроса объекта мониторинга увеличивается, например, в 10 раз, т. е. вместо 1 раза в 5 минут, опрос осуществляют каждые 30 секунд или еще чаще.

Предметом данного исследования является алгоритм и метод выявления нестационарных состояний объекта, на котором проводят измерение. При этом в работе сформулированы и решаются следующие задачи:

символьное кодирования значений временного ряда и способ кодирования участков (ячеек) временного ряда вектором оценок энтропии сдвигов;

метод обучения классификатора состояний объекта измерения на основе энтропии сдвигов;

метода классификации состояния по тестовой выборке измерений, в которых измеряемая характеристика описывается своим распределением вероятностей сдвигов.

### Оценка энтропии кодового слова, описывающего временной ряд наблюдаемой метрики

Для выявления в кодовом слове-строке анализируемого временного ряда «запрещенных» слогов, идентифицирующих развитие аварии воспользуемся оценкой энтропии слов [10].

При этом оценку энтропии кодовых слов описывающего временной ряд наблюдаемого параметра осуществляют в следующем порядке [10]. Сначала фиксируют длину слога  $m$  и алфавит  $\Sigma$ . Множество различных слогов на выбранном алфавите составит  $\Sigma^m$ . Соответственно мощность этого множества  $M = |\Sigma^m|$  составляет общее число слогов. Если обозначить  $k$  – мощность алфавита, то  $M = k^m$ . Для фиксированной длины слогов  $m$  вводится произвольная их нумерация  $i = \overline{1, M}$ , а также счетчики числа слогов  $c_i$ . В ходе анализа временного ряда  $T$  длиной  $n$ , происходит сдвиг временного окна шириной  $m$  на один интервал  $[t_i, t_{i+1}]$ . Таким образом, имеется  $n - m + 1$  позиций временного окна, для каждой из которых идентифицируется слог, полученный в окне. Если в текущей позиции окна шириной  $m$  наблюдается слог, имеющий в принятой нумерации номер  $i = \overline{1, M}$ , то значение счётчика числа слогов  $c_i$  возрастает на единицу. Тогда по полученным значениям счётчика  $c_i$  осуществляется оценка энтропии слов по выражению

$$C_m = -\sum_{i=1}^M \left( \frac{c_i}{n-m+1} \right) \log_m \left( \frac{c_i}{n-m+1} \right) \quad (1)$$

Использование в качестве основания алгоритма мощности различных слогов  $M$  автоматически нормирует значение энтропии слов  $C_m$ . Ситуация, когда  $C(m) = 0$  означает, что все слоги длиной  $m$  одинаковы и состоят из одного и того же слога или при длине слога совпадающим с длиной наблюдаемого кодового слова, т. е.  $m = n$ , мы имеем только один слог. А случай, когда  $C(m) = 1$ , соответствует одинаковой частоте встречаемости всех возможных слогов из  $\Sigma^m$  в наблюдаемом кодовом слове-строке (частота символов алфавита одинакова в исходном кодовом слове).

В результате оценки энтропии слов можно построить функцию  $C(m) = C_m$ , с аргументом  $m$  ( $1 \leq m \leq n$ ), которая вычисляется при фиксированном  $m$  по анализируемому временному ряду в соответствии в выражением (1) и увеличением на единицу ширины окна на области определения  $m$  от 1 до  $n$ .

В соответствии с терминами символической динамики [15], функция  $C(m)$  есть оценка энтропии сдвигов.

Проведем для каждой ячейки процедуру вычисления энтропии сдвигов последовательно с возрастающей шириной окна  $m = 1, \dots, W$ . В результате получим вектор энтропийной характеристики ячейки  $u_i$ :  $h = (C_1, C_2, \dots, C_m)$ .

### Влияние закона распределения параметров временного ряда на прогнозирование отказа

При анализе методов обработки временных рядов нужно помнить, что основным правилом, определяющим выбор конкретного математического аппарата для их анализа при контроле параметров сетевого оборудования, является степень неоднородности объектов мониторинга [16]. В [17] такая степень неоднородности определяется по шкале (например, от 0 до 1, в сторону увеличения неоднородности). Наиболее подходящий математический аппарат, в зависимости от степени неоднородности, определяется, например, методом экспертных оценок (в частности, метод бинарных сравнений). В целом обоснование степени важности сетевого элемента в распределенной сети определяется на основе положений теории важности критериев:

для однотипных сетевых элементов степень неоднородности ограничена значениями от 0 до 0,6. Это объясняется высокой степенью унификации, «схожести» контролируемых сетевых элементов, а также фиксируемым потоком измерительной информации, характеризуемым свойствами однородности. Процесс изменения ТС в однотипных сетевых элементах более плавный, что способствует относительно высокой эффективности процессов обучения и обобщения, например, при использовании искусственных нейронных сетей (ИНС). Здесь процедура оценивания ТС основана на методах экспертных оценок, статистических методах распознавания, метрических методах, методах статистических решений (Неймана-Пирсона, минимакса), а также ИНС [16, 17];

для неоднотипных сетевых элементов (например, периферийного оборудования), отличающихся импульсным, нестационарным характером потока измерительной информации с пуассоновским законом распределения или законом распределения Вейбула («рваный» сигнал, получаемый с большим разбросом), поступающего от объекта мониторинга (при степени неоднородности от 0,7 до 1), наиболее применим метод дискретных вейвлет-преобразований (ДВП), а также метод последовательного анализа Вальда [16,17].

Для моделирования односторонней задержки каналов связи используются следующие распределения вероятностей непрерывных случайных величин [6]:

**Гамма-распределение.** Гамма-распределение асимметрично и определено только для неотрицательных действительных чисел. Оно использует два параметра: параметр формы  $\alpha > 0$  и параметр масштаба  $\beta > 0$ . Варьирование  $\alpha$  изменяет форму функции плотности, в то время как варьирование  $\beta$  соответствует изменению единиц измерения (например, от микросекунд до миллисекунд) при неизменной форме функции плотности. Исследования показали [18], что гамма-распределение во многих ситуациях адекватно приближает задержки маршрутизации.

**Распределение Рэлея.** Распределение Рэлея является простой альтернативой гамма-распределению, которое принимает только один параметр –  $\sigma^2$ . Эта потеря в степени свободы оправдана тем, что рэлеевское распределение по-прежнему показывает аналогичное поведение во многих случаях хотя является довольно грубым приближением к реальному поведению задержки маршрутизации.

Основное преимущество его использования состоит в меньшей вычислительной сложности определения параметра.

*Смещенное гамма-распределение.* Как только оценены параметры гамма-распределения, моделирующего задержку маршрутизации, можно промоделировать поведение полной задержки, включающей также внутреннюю задержку (передачи пакетов по физической среде)  $c$ . Для этого гамма-распределение должно быть дополнено третьим параметром  $c > 0$ , которая сдвигает пик распределение на  $c$  единиц вправо. Это линейное преобразование приводит к распределению, называемому смещенным гамма-распределением. Внутренняя задержка  $c$  независима от состояния маршрутизаторов на пути, которые, в свою очередь, моделируется посредством параметров  $\alpha$  и  $\beta$ .

*Смещенное распределение Рэлея.* Так же, как смещенное гамма-распределение, смещенное распределение Рэлея является обобщением с дополнительным параметром  $c > 0$ , учитывающим внутреннюю задержку.

Функции плотности указанных распределений вероятностей вместе с их математическим ожиданием и дисперсией и графиками функций плотности с несколькими выбранными параметрами, приведены в таблице 1.

Таким образом, проведенный выше качественный обзор научно-методического аппарата анализа временных рядов показал, что каждый из рассмотренных методов имеет свои достоинства и недостатки. В силу наличия временных рядов с регулярными периодическими компонентами в различных сферах науки, решение задачи их прогнозирования является важной и актуальной научно-технической задачей, что подтверждает необходимость формирования самостоятельной методики прогнозирования (превентивной идентификации) аномальной ситуации во временном ряду метрик сетевых элементов распределенной ИТКС, позволяющей в явном виде учесть эти компоненты и отвечающей следующим свойствам:

- инвариантности относительно обрабатываемых метрик разнородных сетевых элементов ИТКС в рамках выбранного класса прогнозируемых процессов;
- учета взаимосвязи сечений не только на интервале периодичности случайного процесса, но также для тренда и его случайной компоненты (центрированного случайного процесса);
- возможности регуляризации временного ряда по большому числу параметров.
- наличия теоретически обоснованного алгоритма оптимизации.

#### Метод обучения классификатора состояний объекта мониторинга на основе энтропии сдвигов

В основе предложенного метода лежит предположение, что любая ячейка исходного временного ряда принадлежит ко всем формируемым состояниям  $C_k$ ,  $k = 1, M$ , но с разной вероятностью. Тогда задача будет заключаться в «подгонке» распределений «смеси состояний» к данным ячеек, а затем в определении вероятностей принадлежности измеренного вектора наблюдения к каждому состоянию.

Построим гистограмму энтропии для каждой компоненты введенного ранее вектора  $h$ . По оси  $x$  изменяется величина энтропии от 0 до 1, а по оси  $y$  – количество ячеек с данной величиной энтропии. Количество интервалов энтропии положим равным  $E$ .

Будем считать, что каждая гистограмма (для каждой компоненты  $h = (C_1, C_2, \dots, C_m)$ ) представляет собой смесь функций Гаусса

$$p(h|\theta) = \sum_{m=1}^K \pi_m \cdot N(h|\mu_m, \sigma_m^2),$$

где  $\pi$  коэффициенты участия компонентов функций Гаусса в смеси, удовлетворяющие свойству  $\sum \pi_k = 1$ . Таким образом,  $p(h)$  представляет собой плотность распределения вероятностей энтропии сдвигов. Для указанной плотности рассмотрим логарифмическую функцию правдоподобия:

$$\begin{aligned} L(\theta) &= \ln \left( \prod_i p(h_i|\theta) \right) = \ln \left( \prod_{i=1}^K \pi_k \cdot N(h_i|\mu_k, \sigma_k^2) \right) = \\ &= \sum_i \ln \left( \sum_{k=1}^K \pi_k \cdot N(h_i|\mu_k, \sigma_k^2) \right), \end{aligned}$$

где  $\theta \in \{\pi_k, \mu_k, \sigma_k^2\}$ ,  $k \in \{1, \dots, K\}$ .

Для максимизации функции продифференцируем ее по параметру  $\mu_k$ .

Для краткости положим  $\phi_k(h_i) = N(h_i|\mu_k, \sigma_k^2)$ ,

$$\begin{aligned} \frac{\partial L(\theta)}{\partial \mu_k} &= \sum_i \frac{1}{\sum_{k=1}^K \pi_k \phi_k(h_i)} \pi_k \frac{\partial \phi_k(h_i)}{\partial \mu_k} = \\ &= \sum_i \frac{\pi_k \cdot \phi_k(h_i)}{\sum_{k=1}^K \pi_k \cdot \phi_k(h_i)} \frac{1}{\phi_k(h_i)} \frac{\partial \phi_k(h_i)}{\partial \mu_k} = \sum_i \frac{\pi_k \cdot \phi_k(h_i)}{\sum_{k=1}^K \pi_k \phi_k(h_i)} \frac{\partial \ln(\phi_k(h_i))}{\partial \mu_k}. \end{aligned}$$

Значение  $\partial \ln \phi_k(x_i) / \partial \mu_k$  представляет собой производную логарифмической функции правдоподобия функции Гаусса и может быть использовано для установления параметров несмешанной модели. Наибольшие сложности при нахождении максимума вызывают множители  $\frac{\pi_k \phi_k(x_i)}{\sum_k \pi_k \phi_k(x_i)}$  также

зависящие от переменных.

Введем скрытую переменную  $z \in \{1, \dots, K\}$ , указывающую, что данная точка  $h$  пришла из  $k$ -го гауссиана. Тогда определим,

$$p(z = k) = \pi_k,$$

$$p(h|z = k) = \pi_k N(h|\mu_k, \sigma_k^2),$$

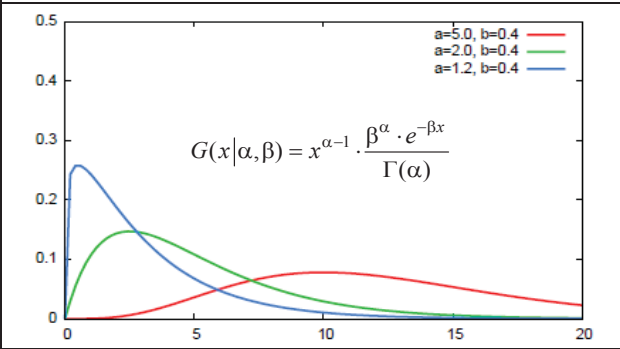
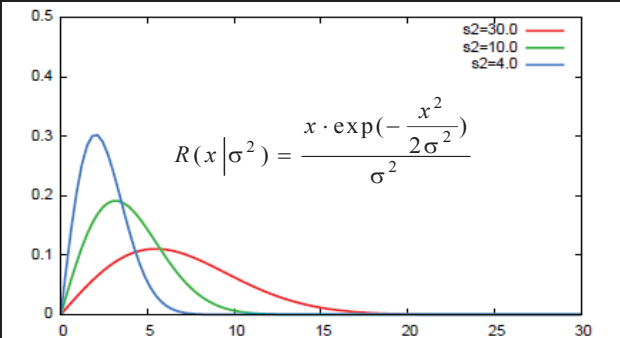
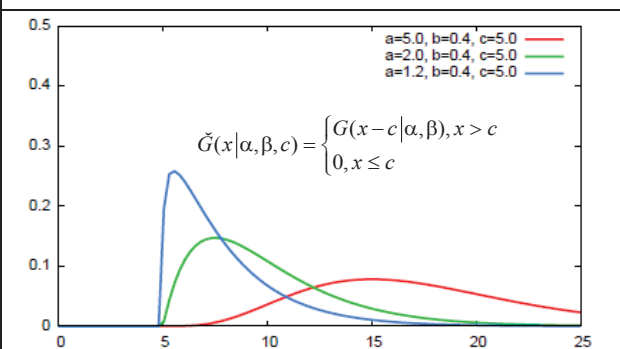
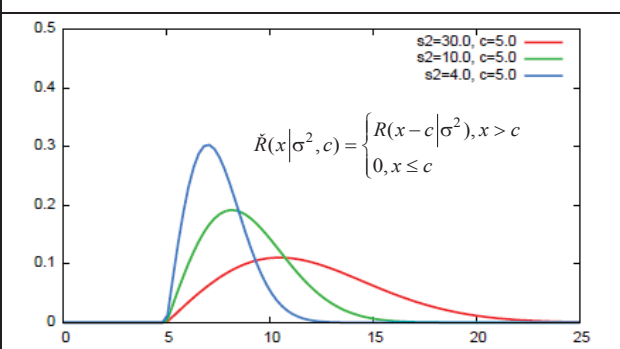
$$p(h) = \sum_{k=1}^K p(h|z = k) = \sum_{k=1}^K \pi_k N(h|\mu_k, \sigma_k^2).$$

Это разлагает гауссову смесь на скрытую переменную  $z$  и параметры модели  $\theta$ , которые позволяют выяснить, из какого гауссова значения была получена каждая точка данных. При этом вероятность получения точки из  $k$ -го гауссиана равна

$$p(z = k|h, \theta) = \frac{p(h, z = k; \theta)}{\sum_k p(h, z = k; \theta)}.$$

Таблица 1

Распределения вероятностей, используемые для моделирования поведения односторонней задержки

Распределение	Функция плотности	Область значений	Математическое ожидание	Дисперсия
Гамма-распределение	 $G(x \alpha, \beta) = x^{\alpha-1} \cdot \frac{\beta^\alpha \cdot e^{-\beta x}}{\Gamma(\alpha)}$	$[0, \infty)$	$\frac{\alpha}{\beta}$	$\frac{\alpha}{\beta^2}$
Распределение Рэлея	 $R(x \sigma^2) = \frac{x \cdot \exp(-\frac{x^2}{2\sigma^2})}{\sigma^2}$	$[0, \infty)$	$\sigma \sqrt{\frac{\pi}{2}}$	$\frac{4-\pi}{2} \sigma^2$
Смещенное гамма-распределение	 $\check{G}(x \alpha, \beta, c) = \begin{cases} G(x-c \alpha, \beta), & x > c \\ 0, & x \leq c \end{cases}$	$[0, \infty)$	$\frac{\alpha}{\beta} + c$	$\frac{\alpha}{\beta^2}$
Смещенное распределение Рэлея	 $\check{R}(x \sigma^2, c) = \begin{cases} R(x-c \sigma^2), & x > c \\ 0, & x \leq c \end{cases}$	$[0, \infty)$	$\sigma \sqrt{\frac{\pi}{2}} + c$	$\frac{4-\pi}{2} \sigma^2$



Указанная величина может выступать весовым коэффициентом в рассмотренной производной функции правдоподобия. Если мы знаем  $z$ , т. е. из какого гауссовского значения получены данные, нам больше не нужно суммировать по всем  $K$  гауссианам ( $\sum p(x, z)$ ), чтобы максимизировать предельную вероятность. Вместо этого рассматриваем на каждом подмножестве  $x$ , исходящем из  $k$ -го гауссиана, и можем оценить  $\theta_k$  как

$$\arg \max_{\theta_k} \sum_i \ln p(h_i; \theta_k) \forall i (z_i = k).$$

Если мы знаем, по какой гауссовой компоненте была получена точка данных (скрытая переменная  $z$ ), то мы можем максимизировать логарифмическую вероятность и получить оценки параметров модели. В свою очередь, если известны параметры модели, можно вычислить апостериорную вероятность  $z$ , которая позволит оценить, из какого гауссова значения пришла каждая точка данных. Вместо того, чтобы одновременно вычислять оптимальную скрытую переменную  $z$  и параметр модели  $\theta$ , мы по очереди будем оптимизировать каждую из них, до нахождения точной оценки. Указанные соображения позволяют использовать для разделения смеси распределений энтропии сдвигов *EM*-алгоритм [19], состоящий из следующих двух шагов:

*E-шаг.* На каждом *E*-шаге вычислим текущие вероятности принадлежности точек  $h$   $k$ -й компоненте распределения вероятностей энтропии по формуле:

$$z_{ik} = \frac{\pi_k N(h_i | \mu_k, \sigma_k^2)}{\sum_m \pi_m N(h_i | \mu_m, \sigma_m^2)}.$$

*M-шаг.* На каждом *M* шаге вычисляются новые оценки параметров  $\mu_k, \sigma_k^2$  путем максимизации нижней оценки  $Q(\theta)$  приведенной выше логарифмической функции правдоподобия  $L(\theta)$ , полученной из условия выпуклости  $L(\theta)$  путем применения неравенства Йенсена с подстановкой соответствующих параметров, вычисленных на предыдущем шаге.

$$Q(\theta; \theta^t) = \sum_i \sum_k z_{ik} \ln(\pi_k \cdot N(h_i | \mu_k, \sigma_k^2)).$$

Найдя частные производные указанного выражения:

$$\frac{\partial Q(\theta; \theta^t)}{\partial \mu_k} = 0, \quad \frac{\partial Q(\theta; \theta^t)}{\partial \sigma_k^2} = 0, \quad \frac{\partial Q(\theta; \theta^t)}{\partial \pi_k} = 0,$$

получим выражения для обновления текущих значений:

$$\mu_k^{(e+1)} = \frac{\sum_{i=1}^n z_{ik}^{(t)} h_i}{\sum_{i=1}^n z_{ik}^{(t)}}, \quad \sigma_k^{2(t+1)} = \frac{\sum_{i=1}^n z_{ik}^{(t)} (h_i - \mu_k^{(t+1)})^2}{\sum_{i=1}^n z_{ik}^{(t)}}.$$

Результирующее правило обновления для  $\pi_k$  идентично для любого типа смешанных моделей и может быть определено как:

$$\pi_k = \frac{1}{n} \sum_{i=1}^n z_{ik} = \frac{N_k}{n},$$

где  $N_k$  – ненормализованный вес компонента  $k$ :  $N_k = \sum_{i=1}^n z_{ik}$ .

$$\text{Тогда } \pi_k^{(t+1)} = \frac{\sum_{i=1}^n z_{ik}^{(t)}}{n}.$$

### Классификация состояния сетевого устройства

После определения параметров распределения вероятностей для каждого из состояний  $C_k, k = \overline{1, M}$  для оперативной оценки текущего состояния объекта измерений можно использовать теорему Байеса.

Допустим, в процессе измерения была получена выборка  $X = (x_1, x_2, \dots, x_n)$ . К указанной выборке производится добавление «хвоста», –  $l$  измерений, полученных на предыдущих шагах. К полученной в результате выборке  $X = (x_1, x_2, \dots, x_l, \dots, x_{l+n})$  применяется процедура разбики на ограниченное число ячеек  $u_i$  с вычислением в каждой из них вектора энтропии сдвигов  $h(u_i)$ , рассмотренного выше.

В результате полученный набор векторов энтропии сдвигов по каждой их проекции (обозначим ее как случайную величину  $H$ ) проверяется на принадлежность к каждому из состояний на основании апостериорных вероятностей  $P(C=k|H)$ .

Формально правило классификации может быть выражено как:  $H \sim C_k \Leftrightarrow k = \arg \max_i P(C = i | H)$ .

Иными словами,  $X$  принадлежит к классу  $C_k$ , если апостериорная вероятность  $P(C=k|H)$  максимальна.

Предполагая, что  $n$  измерений выборки  $X$  независимы и распределены одинаково получаем вероятности принадлежности выборки  $H = (h_1, \dots, h_n)$  состояниям  $C_k$ :

$$P(H|C = k) = \prod_{i=1}^n N(h_i | \mu_k, \sigma_k^2).$$

Априорные вероятности  $P(C = k)$  для  $M$  состояний  $C_k, k = \overline{1, M}$ , будем полагать одинаковыми:

$$P(C = k) = \frac{1}{M}.$$

Вероятность  $P(C = k|H)$  того, что, полученная проекция энтропии  $H$  была произведена  $k$ -й компонентой можно определить через теорему Байеса:

$$P(C = k|H) = \frac{P(H|C = k)P(C = k)}{P(H)} = \frac{P(H|C = k)P(C = k)}{\sum_i P(H|C = i)P(C = i)}.$$

Полученный в результате набор вероятностей принадлежности состояниям при помощи логических правил принятия решений используется для генерации событий операционной системы мониторинга.

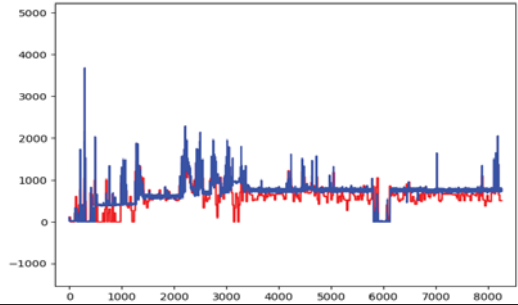
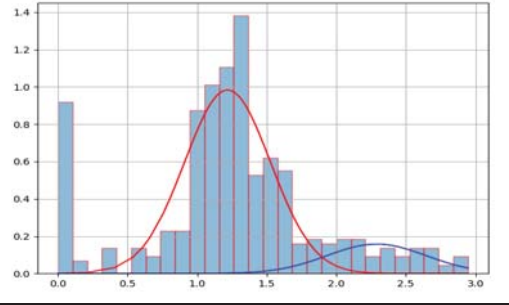
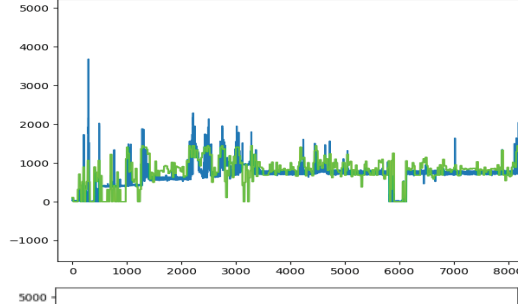
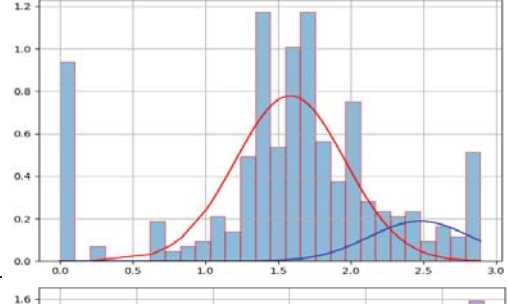
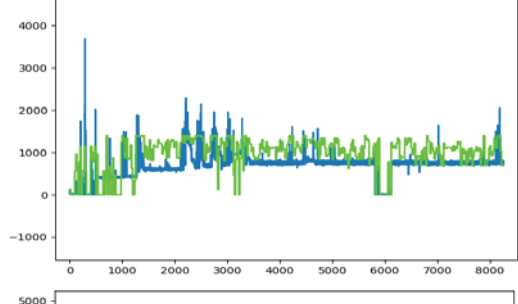
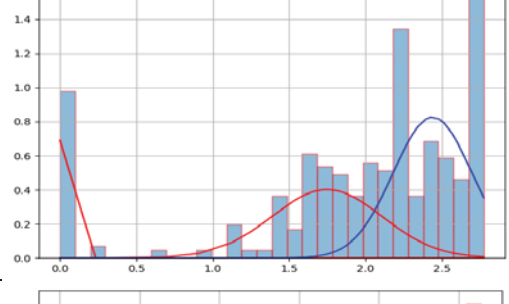
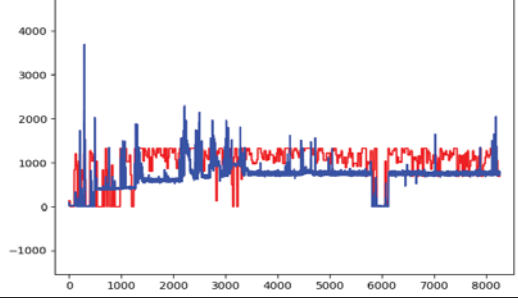
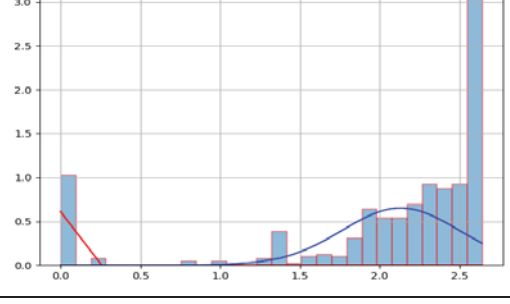
Для исследования качества процесса классификации состояния сетевого устройства по предложенному алгоритму на основе статистики энтропии сдвигов был поставлен эксперимент на основе упомянутого набора данных недельной загрузки процессора сервера виртуализации.

Результаты эксперимента показаны в табл. 2. Здесь для фиксированного интервала (50) точек наблюдения временного ряда (синий цвет на левых рисунках табл. 2) и окон вычисления энтропии размером 2, 3, 5 и 7 была вычислена статистика энтропии сдвигов (красный и зеленый цвет на левых рисунках табл. 2), в виде гистограмм (правые рисунки табл. 2), которые аппроксимированы тремя нормальными распределениями *EM*-алгоритмом, описанном выше, со следующими значениями параметров математического ожидания (**m**) и дисперсии (**D**):

– для ширины скользящего окна – 2: **m**: 0; 1.23; 2.29, **D**: 0.13; 0.09; 0;

Таблица 2

Результаты эксперимента

Параметры	Временной и энтропийный ряды	Гистограмма и параметры смешанного распределения	Исходные данные
Интервал 50 Окно 2			<b>m:</b> 0; 1.23; 2.29. <b>D:</b> 0.13; 0.09; 0.
Интервал 50 Окно 3			<b>m:</b> 0; 1.58; 2.48. <b>D:</b> 10 <sup>-6</sup> ; 0.15; 0.12.
Интервал 50 Окно 5			<b>m:</b> 0.02; 1.70; 2.41. <b>D:</b> 0.07; 0.003; 0.12.
Интервал 50 Окно 7			<b>m:</b> 0.01; 2.13; 2.63. <b>D:</b> 10 <sup>-5</sup> ; 0.01; 0.1.

– для ширины скользящего окна – 3; **m:** 0; 1.58; 2.48,  
**D:** 10<sup>-6</sup>; 0.15; 0.12;  
– для ширины скользящего окна – 5; **m:** 0.02; 1.70; 2.41,  
**D:** 0.07; 0.003; 0.12;  
– для ширины скользящего окна – 7; **m:** 0.01; 2.13; 2.63,  
**D:** 10<sup>-5</sup>; 0.01; 0.1. Таким образом, как видно из таблицы 2, наиболее четкое разделение состояний (без нагрузки, переходное состояние, перегрузка) наблюдается для энтропийных окон шириной 2 и 3.

С возрастанием размера скользящего окна качество аппроксимации визуально ухудшается, что затрудняет процесс классификации состояния сетевого устройства.

Описанный подход с классификацией состояния элементов телекоммуникационной сети неплохо работает в случае возможности выделения классов поведений. Это было продемонстрировано для односторонней задержки [20], когда компонента, связанная с маршрутизацией (ожидание в очередях), включается в общее выражение задержки лишь при средних и высоких нагрузках. В меньшей степени этот метод может быть использован для оценки состояния загрузки вычислительных ресурсов, в частности процессора. Хотя и здесь имеет место задержка, связанная с переключением контекста вычисления, но она более связана с организацией вычислительного процесса, чем с режимом нагрузки.

В этом случае требуется предварительный этап уточнения числа состояний и соответствующих им распределений. Это продемонстрировано на рисунках табл. 2, где приведена попытка аппроксимации гистограммы статистики недельной загрузки процессора сервера виртуализации двумя и тремя нормальными распределениями по смешанной гауссовской модели *EM*-алгоритмом.

Последовательность действий на этапе обучения классификатора с использованием процедуры *EM*-алгоритма, а также при выполнении этапа классификации состояния сетевого элемента представлено на рисунке 5. Данные этапы включаются в общую методику превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик.

### Алгоритм превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик

Исходя из рассмотренных методов анализа временных рядов предложен алгоритм превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик.

Блок-схема алгоритма состоит из четырех этапов: предварительного этапа, этапа кодирования временных рядов, этапа идентификации состояния сетевого элемента и завершающего этапа (рис. 6).

#### Предварительный этап

**Ввод исходных данных:** о составе ИТКС; структуре ее децентрализованной подсистемы мониторинга (матрица тяготений серверов мониторинга к сетевым элементам); наблюдаемых параметрах сетевых элементов; величинах эксплуатационных допусков на параметры сетевых элементов, а также значениях профилактических допусков на них для различных режимов функционирования и условий эксплуатации сетевых элементов [12]; режимах мониторинга (активный, пассивный) и периодичности опроса сервером мониторинга сетевых элементов; значениях ошибок первого и второго рода ( $\alpha$  – «ложной тревоги» и  $\beta$  – «пропуск отказа», соответственно); классах (видах) технического состояния сетевого элемента; используемых протоколах сбора измерительной информации и др.

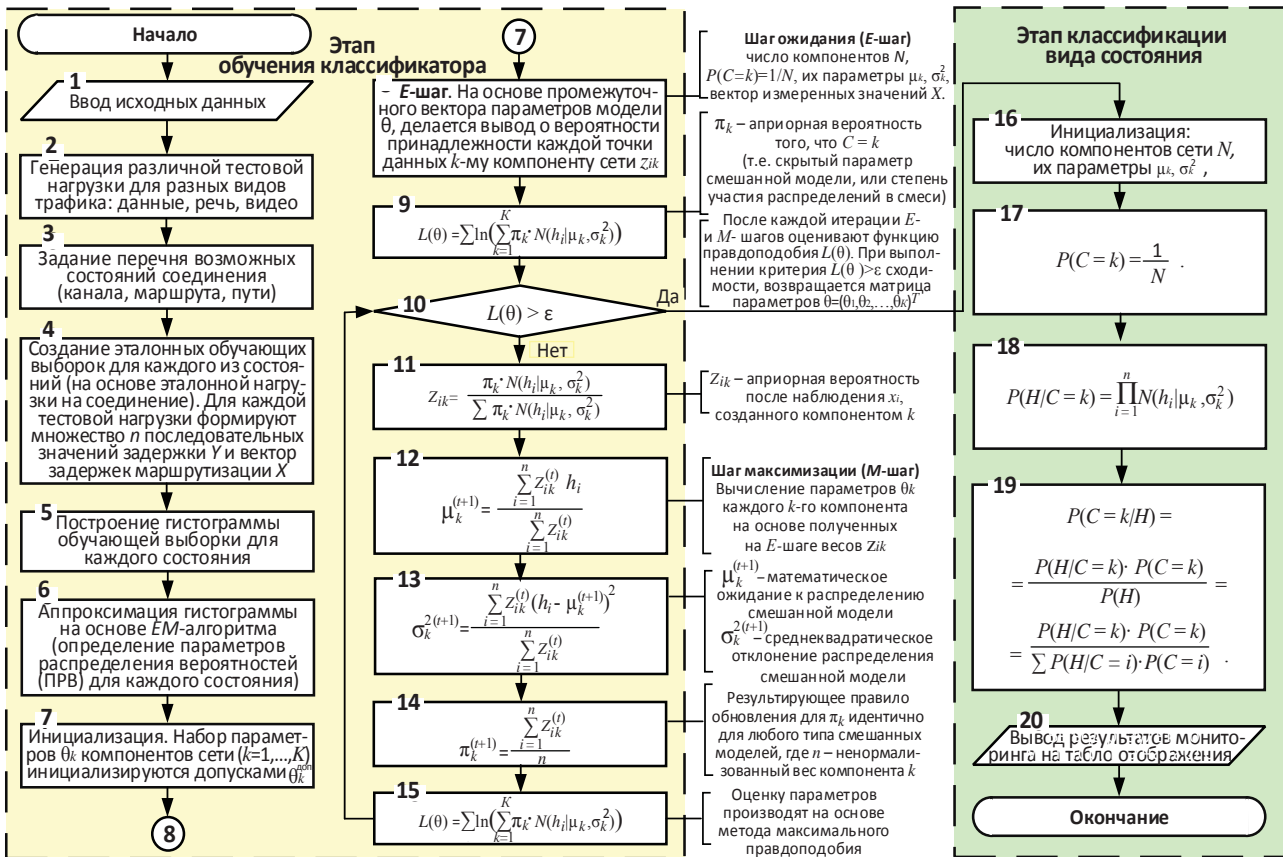


Рис. 5. Обучение классификатора с использованием *EM*-алгоритма и определение вида состояния

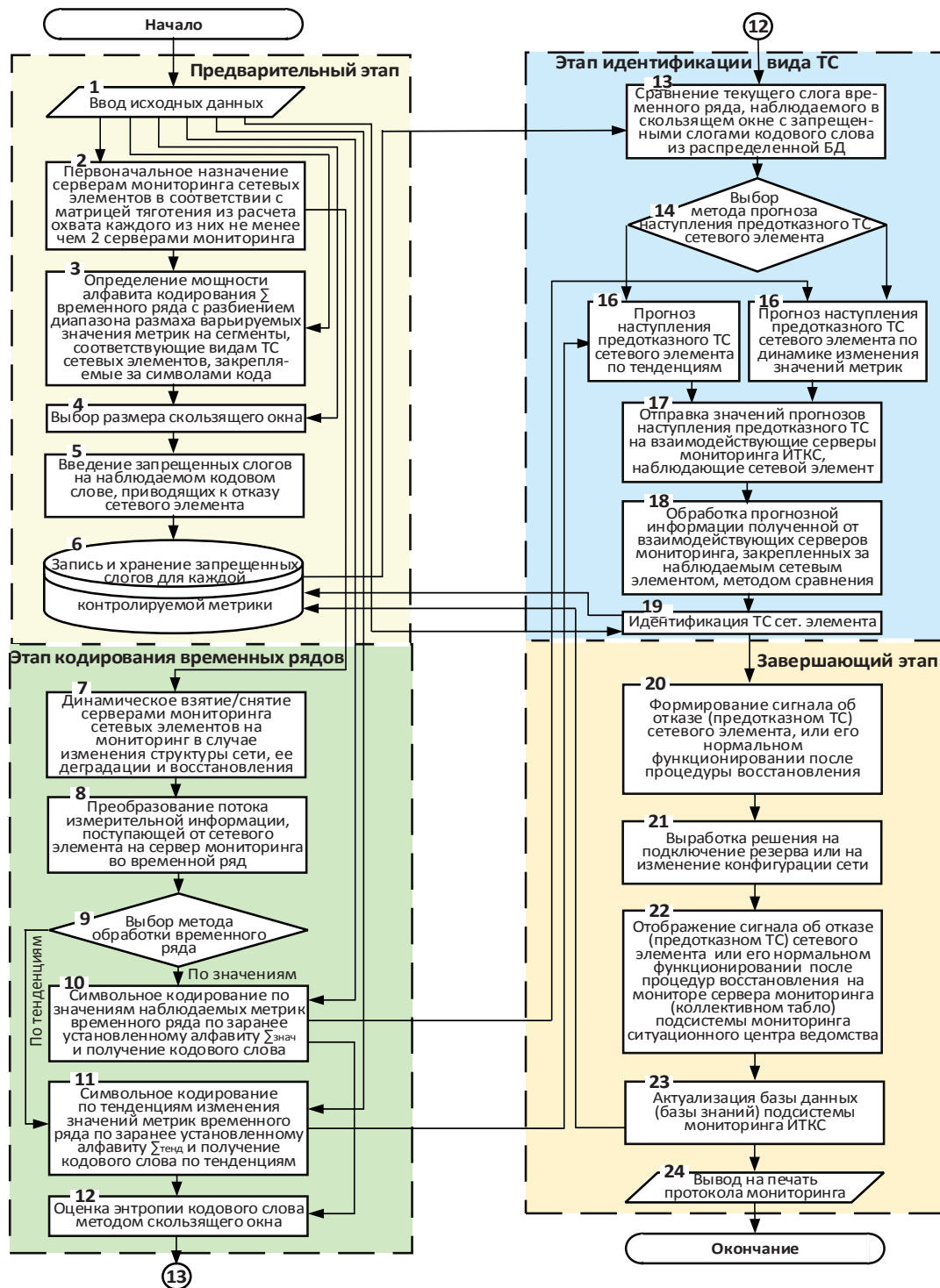


Рис. 6. Блок-схема алгоритма превентивной идентификации аномального состояния сетевого элемента на временных рядах его метрик

Первоначальное назначение серверам мониторинга сетевых элементов для наблюдения их ТС (мониторинга) в соответствии с матрицей тяготения серверов к сетевым элементам из расчета охвата каждого сетевого элемента не менее чем двумя серверами мониторинга.

Определение мощности алфавита кодирования временного ряда с разбиением диапазона размаха варьируемых значений

метрики на сегменты, соответствующие классам (видам) технического состояния сетевых элементов, закрепляемые за символами кода. Соотнесение классов (видов) ТС с символами выбранного алфавита  $\Sigma$  кодирования временного ряда.

Выбор размера скользящего окна. Для каждого эксплуатационного параметра отдельного сетевого элемента данный выбор индивидуален. Важно ширину скользящего окна иметь



таковой, чтобы не пропустить нарастание аварийной ситуации в различных режимах и условиях эксплуатации сетевого элемента, а также минимизировать ошибки первого рода ( $\alpha$ ) «ложный отказ» и второго рода ( $\beta$ ) «пропуск отказа». Выбор размера скользящего окна, как правило, осуществляется на этапе испытаний или подконтрольной эксплуатации сетевого элемента.

*Введение запрещенных слогов* на наблюдаемом кодовом слове-строке, приводящих к отказу. Первоначально состав запрещенных слогов определяется в ходе испытаний и подконтрольной эксплуатации для различных режимов функционирования и условий эксплуатации сетевого оборудования, а в последующем – в соответствии нарабатываемой статистикой на основных этапах жизненного цикла ИТКС. Поэтому этапу испытаний и подконтрольной эксплуатации должно уделяться важное значение.

*Запись и хранение запрещенных слогов* для каждой контролируемой метрики каждого сетевого элемента в распределенной базе данных (базе знаний – БЗ) ИТКС, их обновление и репликация в соответствии с надежностью функционирования ИТКС и статистикой эксплуатации сетевых элементов на основных этапах их жизненного цикла.

#### **Этап кодирования временных рядов**

*Динамическое взятие/снятие серверами мониторинга сетевых элементов на мониторинг* в случае изменения структуры сети, ее деградации или восстановления, из расчета охвата каждого сетевого элемента не менее чем двумя серверами мониторинга. Такое динамическое распределение одновременно должно модифицироваться любым из участвующих серверов для поддержки выполнения условия обеспечения  $\sum_{i=1}^{M_{\max}} m_i \geq 2$  минимального количества серверов мониторинга (не менее двух) на одно сетевое устройство.

*Преобразование потока ИИ*, поступающей от сетевого элемента в сервер мониторинга во временном ряду, а также выбор вида временного ряда и типа средств его визуализации.

*Выбор метода обработки временного ряда* – символьное кодирование по значениям или символьное кодирование по тенденциям.

*Символьное кодирование значений* наблюдаемых метрик временного ряда в соответствие с символами ранее установленного алфавита  $\Sigma_{\text{знач}}$  и получение кодовых слов-строк по значениям.

*Символьное кодирование по тенденциям* изменения значений метрик временного ряда символами ранее установленного алфавита  $\Sigma_{\text{тенд}}$  и получение кодовых слов-строк по тенденциям.

*Оценка энтропии кодового слова.* Изначально позиционированное в начале наблюдаемого кодового слова-строки длиной  $n$ , скользящее окно шириной  $t$  сдвигается каждый раз на один символ (временной такт)  $t_{i+1}$ . Для каждого его  $n - t + 1$  положения распознается слог кодового слова, полученный в скользящем окне. Если в текущей позиции скользящего окна шириной  $t$  наблюдается слог, имеющий номер  $i$  в принятой нумерации, то значение счетчика  $c_i$  увеличивается на единицу. Расчет оценки энтропии слов  $S_m$  проводится по выражению (1).

#### **Этап идентификации состояния сетевого элемента**

*Сравнение* текущего слога временного ряда, наблюдаемого в скользящем окне с запрещенными слогами кодового слова, записанными в распределенной базе данных (базе знаний), предполагает поиск (фильтрацию) запрещенных слогов в наблюдаемом кодовом слове-строке временного ряда.

*Выбор метода прогноза* наступления предотказного ТС сетевого элемента.

*Прогноз* наступления предотказного состояния сетевого элемента *по тенденциям* их изменения (выявление опасных тенденций). В случае идентификации опасных трендов развития аварии необходимо увеличить частоту опроса сетевого элемента с целью не допустить пропуска отказа и минимизировать ошибку второго рода  $\beta$ .

В данном алгоритме процедура увеличения скважности опроса сетевого элемента серверов мониторинга при выявлении предотказного технического состояния не представлена, решается программно отдельным блоком алгоритма.

*Прогноз* наступления предотказного состояния сетевого элемента по динамике изменения значений метрик в наблюдаемых слогах ключевых слов анализируемого ряда временного ряда. В случае идентификации предотказного состояния сетевого элемента доступная измерительная информация (величины значений наблюдаемой метрики) сверяется не только с эксплуатационным допуском на параметр, но и с профилактическим допуском, зависящим от конкретного режима функционирования и условий эксплуатации сетевого элемента.

*Отправка значений прогнозов* наступления предотказного состояния на серверы мониторинга, взаимодействующие в ИТКС и наблюдающие сетевой элемент. При этом если на сервере мониторинга, спрогнозировавшим предотказное состояние доступна измерительная информация инструментального контроля, то на взаимодействующие серверы мониторинга передается только прогнозное значение в виде символьной записи (типа  $\{+++ \}$ , или  $\{ABE\}$ ).

*Обработка прогнозной информации*, полученной на шагах прогноза и поступающей от взаимодействующих серверов мониторинга ИТКС, закрепленных за наблюдаемым сетевым элементом, методом сравнения (с использованием мажоритарного принципа и пр.), а также сопоставления действующих режимов его функционирования и условий эксплуатации (выявление причин наступления предотказного состояния).

*Идентификация технического состояния* сетевого элемента по конечному символу текущего слога наблюдаемого кодового слова временного ряда.

#### **Завершающий этап**

*Формирование сигнала об отказе*, предотказном ТС или иной аномалии сетевого элемента, или его нормальном функционировании после процедур восстановления (устранения отказа).

*Выработка решения на подключение резерва* или на изменение конфигурации сети в связи с отказом/восстановлением сетевого элемента. Для повышения оперативности данный шаг выполняется параллельно с предыдущим.

*Отображение сигнала об отказе* (предотказном ТС) сетевого элемента или его нормальном функционировании после процедур восстановления (устранения отказа) на мониторе сер-

вера мониторинга (коллективном табло) подсистемы мониторинга.

*Актуализация базы данных* (базы знаний) о ТС сетевых элементов ИТКС, обновление структуры сети в связи с последними изменениями (отказом, резервирование, восстановлением), динамическое перезакрепление серверов мониторинга за сетевыми элементами в связи с динамикой изменения ТС ИТКС (изменение матрицы тяготения серверов мониторинга и сетевых элементов), уточнение исходных данных, обновление и репликация распределенной БД ИТКС.

*Вывод на печать* протоколов мониторинга.

### Модельный пример

Описанный в методике подход с классификацией состояний элементов телекоммуникационной сети неплохо работает в случае возможности выделения классов поведений. Это было продемонстрировано для односторонней задержки [20], когда компонента, связанная с маршрутизацией (ожидание в очередях), включается в общее выражение задержки лишь при средних и высоких нагрузках. В меньшей степени этот метод может быть использован для оценки состояния загрузки вычислительных ресурсов, в частности процессора. Хотя и здесь имеет место задержка, связанная с переключением контекста вычисления, но она более связана с организацией вычислительного процесса, чем с режимом нагрузки. В этом случае требуется предварительный этап уточнения числа состояний и соответствующих им распределений. Это было продемонстрировано в ходе выполненного эксперимента, результаты которого приведены на рисунках 7 и 8.

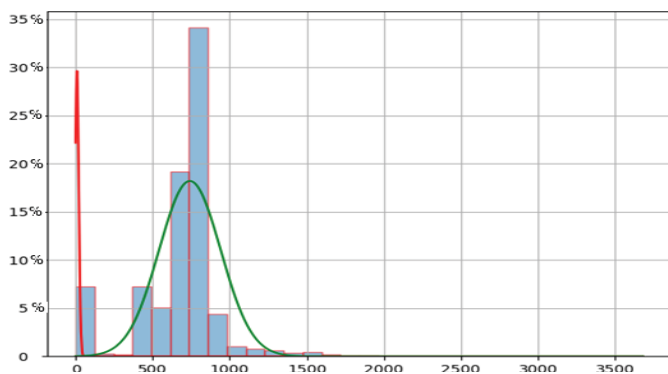


Рис. 7. Аппроксимация гистограммы загрузки процессора двумя нормальными распределениями

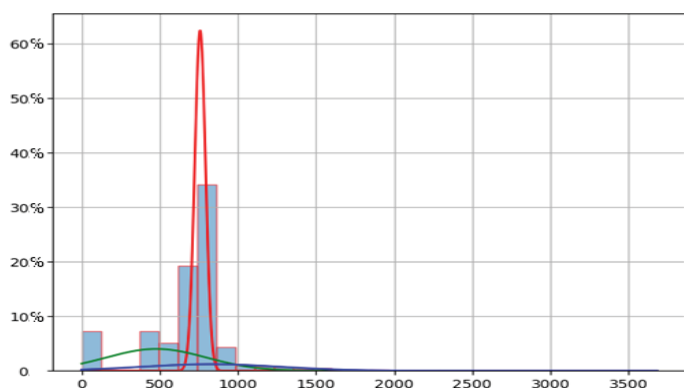


Рис. 8. Аппроксимация гистограммы загрузки процессора тремя нормальными распределениями

Проведя анализ аппроксимации гистограмм загрузки процессора несколькими распределениями выбранных параметров, можно сделать вывод, что наиболее информативна аппроксимация гистограмм наблюдаемых параметров (метрик) сетевых устройств, с двумя нормальными распределениями.

Эксперимент проводился на гистограммах статистики недельной загрузки процессора сервера виртуализации двумя и тремя нормальными распределениями по смешанной гауссовской модели *EM*-алгоритмом. Гистограммы были получены на том же наборе данных, что было использовано для установления оптимальной величины окна для расчета энтропии сдвигов.

Как следует из рисунков, предобработка данных энтропией сдвигов позволяет «разнести» распределения, моделирующие состояния, что обеспечивает более точную их классификацию. При этом хорошо видно, что две компоненты обеспечивают более точную классификацию технического состояния сетевого устройства (рис. 7), нежели три (рис. 8). Эксперимент проводился на параметрах загрузки процессора (тактах).

### Заключение

В работе предложен подход к формированию методики прогнозирования аномальных ситуаций по результатам мониторинга функционального состояния сетевых элементов ИТКС ОП. При этом превентивная идентификация аномального состояния сетевого элемента осуществляется путем выявления «запрещенных» кодовых комбинаций при наблюдении временных рядов, обработанных заимствованными из биоинформатики методами символической динамики, используемыми ранее в процессе анализа сложных нуклеотидных геномных последовательностей, а также введение особого режима мониторинга, когда при идентификации предотказного ТС скважность опроса сервером мониторинга сетевого элемента значительно увеличивается с целью своевременного принятия превентивных управляющих воздействий на сетевую инфраструктуру для недопущения пропуска отказа сетевого элемента или наступления аварии.

В основу предложенного алгоритма заложен метод символического представления временных рядов, на базе которого дана оценка энтропии кодовых слов, описывающих временной ряд наблюдаемой метрики функционирующего сетевого элемента и разработан алгоритм методики идентификации аномальной ситуации на временном ряду его параметров, состоящий из четырех этапов: предварительного этапа, этапа кодирования временных рядов, этапа идентификации вида технического состояния сетевого элемента и завершающего этапа. Данный алгоритм позволит в последующем сформировать порядок функционирования сервера мониторинга для идентификации аномалий в работе ИТКС ОП.

### Литература

1. Легков К. Е., Буренин А. Н. Модели и методы оперативного мониторинга информационных подсистем перспективных автоматизированных систем управления // *Информация и космос*. 2016. № 4. С. 46-60.

2. *Легков К. Е.* Модели и методы мониторинга параметров, характеризующих состояние инфокоммуникационной системы специального назначения // Т-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 1. С. 11-18.

3. *Буренин А. Н., Легков К. Е., Емельянов А. В.* Основные положения системного анализа и подход к построению модели информационной подсистемы инфокоммуникационной подсистемы специального назначения // Системы синхронизации, формирования и обработки сигналов. 2016. Т. 7. № 3. С. 17-23.

4. *Игнатов Н. А.* Прогнозирование временных рядов с регулярными циклическими компонентами с помощью модели периодически коррелированных случайных процессов // Научные труды: Институт народнохозяйственного прогнозирования РАН, 2011. С. 461-477.

5. *Сухопаров М. Е., Лебедев И. С.* Модели анализа функционального состояния элементов устройств сетей и телекоммуникаций «Индустрии 4.0». СПб.: Политех-Пресс, 2020. 121 с.

6. *Васильев Н. В., Забродин О. В., Яшин А. И.* Автоматизированный программный комплекс оценки качества обслуживания в телекоммуникационной сети // Техника средств связи. 2018. № 3 (143). С. 56-61.

7. *Витяев Е. Е., Дергилев А. И., Чадаева И. В., Васикин Ю. Ю., Спицина А. М., Кулакова Е. В., Вишневицкий О. В., Орлов Ю. Л.* Поиск регулярных контекстных сигналов в геномной ДНК / Сб. науч. трудов конференции «Информатика-2016» (Москва, 24-29 апреля 2016 г.). М.: Национальный исследовательский ядерный университет "МИФИ", 2016. С. 52-62.

8. Математические методы для анализа последовательностей ДНК. М.: Мир, 1999. 349 с.

9. *Ульянов М. В., Сметанин Ю. Г.* Об одном характеристическом функционале слов над конечным алфавитом // Информационные технологии. 2017. Т.23. № 5. С.333-341.

10. *Седакин И., Ульянов М. В.* Эффективный по времени алгоритм расчета обобщенной энтропии двумерных слов методом скользящего окна // Современные информационные технологии и ИТ-образование. 2018. Т. 14. № 3. С. 560-566.

11. *Петрушин В. Н., Ульянов М. В.* Бикритериальный метод построения гистограмм // Информационные технологии и вычислительные системы. 2012. № 4. С. 22–31.

12. *Абрамов О. В.* Планирование профилактических коррекций параметров технических устройств и систем // Информатика и системы управления. 2017. № 3 (53). С. 55-66.

13. *Грабуств П.* Способы оценок сходства временных рядов // Научные труды Международной НТК «Теория вероятностей, случайные процессы, математическая статистика и приложения» (Минск, БГУ, 15-19 сентября 2008 г.). Минск: Белорусский государственный университет, 2008. С. 23-24.

14. *Сметанин Ю. Г., Ульянов М. В., Пестова А. С.* Энтропийный подход к построению меры символического разнообразия и его применение к кластеризации геномов растений // Математическая биология и биоинформатика. 2016. Т. 11. № 1. С. 114-126.

15. *Lind D., Marcus B.* *An introduction to symbolic dynamics and coding.* Cambridge, UK: Cambridge University Press, 1995. 495 p.

16. *Винограденко А.М.* Методология интеллектуального контроля технического состояния автоматизированной системы связи специального назначения. Монография. – СПб.: Научно-технические технологии, 2020. – 180 с.

17. *Подюновский В.В.* Идеи и методы теории важности критериев в многокритериальных задачах принятия решений. М.: Наука, 2019. 103 с.

18. *Holleczeck T.* Statistical Analysis of IP Performance Metrics in International Research and Educational Networks. Nuremberg. 2008. Pp. 105-114.

19. *Королев В. Ю., Шевцова И. Г.* Байесовские методы анализа больших данных. М.: ООО «МАКС Пресс», 2020. 140 с.

20. *Аллакин В. В.* Анализ методов оценки временных рядов серверов мониторинга информационно-телекоммуникационной сети общего пользования // Техника средств связи. 2021. № 2 (154). С. 60-80.

21. *Аллакин В. В., Будко Н. П., Васильев Н. В.* Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. 2021. № 3. С. 125-227. DOI: 10.24412/2410-9916-2021-4-125-227.

## THE METHOD OF PREVENTIVE IDENTIFICATION OF THE STATE OF MONITORING OBJECTS BASED ON THE SYMBOLIC REPRESENTATION OF TIME SERIES OF THEIR METRICS

VLADIMIR V. ALLAKIN

St. Petersburg, Russia, vladimir@duduh.ru

**KEYWORDS:** monitoring server, identification of technical condition, special monitoring mode, time series, preventive identification.

### ABSTRACT

**Introduction:** based on the analysis of methods for estimating time series of observed parameters of devices of public information and telecommunications networks, to develop a method for preventive identification of the state of monitoring objects using a symbolic representation of time series of their metrics. **Purpose:** of the study is to determine the generalized universal characteristics of the time series, according to which it is possible to evaluate the variety of observed values of metrics related to a certain area of the state of the monitoring object (the class of its technical condition). **Results:** preventive identification of the abnormal state of the network element is carried out by identifying "forbidden" code syllables on the code word describing the observed time series of the metric. This approach to time series processing is borrowed from symbolic dynamics, which is used in bioinformatics when analyzing complex nucleotide genomic sequences. As a generalized universal characteristic of the time series, the entropy of code words is used, describing the time series encoded by the method of symbolic representation of the data of the observed metrics. An algorithm of the method

of preventive identification of an abnormal situation on a time series of its parameters is developed, consisting of four stages: at the first stage, the time series is symbolically encoded according to possible parameter values; at the second, the entropy of the code word describing the time series of the observed metric is estimated; at the third, the classifier of the states of the measurement object is trained based on the entropy of shifts; at the fourth stage, the state is classified according to a test sample of measurements, in which the measured characteristic is described by its law of probability distribution of shifts. **Practical relevance:** when an abnormal functional state of a network element is detected, a transition to a special monitoring mode is carried out, when the frequency of polling by the monitoring server of the network element is significantly increased in order to timely take preventive control actions on the network infrastructure and prevent failure (the occurrence of an accident). **Discussion:** the methodology will allow to form the order of operation of the monitoring server in the future to identify the functional state of the network element and the public information and telecommunications network as a whole.



## REFERENCES

1. Legkov K. E., Burenin A. N. (2016). Models and methods for monitoring of information subsystems of prospective automated control systems. *Information and Space*. No. 4. Pp.46-60. (in Russian).
2. Legkov K. E. (2016). Models and methods of monitoring parameters characterizing the state of the infocommunication systems a special purpose. *T-Comm*. Vol. 10. No.1, pp. 11-18. (in Russian).
3. Burenin A. N., Legkov K. E., Emelyanov A. V. (2016). The main provisions of system analysis and an approach to building a model of an information subsystem of a special purpose infocommunication subsystem. *Synchronization systems, signal generation and processing*. Vol. 7. No. 3. Pp. 17-23. (in Russian).
4. Ignatov N. A. (2011). Prognozirovaniye vremennykh ryadov s regul'yarnymi ciklicheskimy komponentami s pomoshch'yu modeli periodicheski korrelirovannykh sluchajnykh processov [Prediction of time series with regular cyclical components using the model of a periodically correlated random processes]. *Nauchnye trudy: Institut narodno-hozyajstvennogo prognozirovaniya RAN* [Scientific works: Institute of National Economic Forecasting of the Russian Academy of Sciences]. Pp. 461-477. (In Russian)
5. Suhoparov M. E., Lebedev I. S. (2020). Modeli analiza funktsional'nogo sostoyaniya elementov ustrojstv setej i telekommunikacij "Industrii 4.0" [Model analysis of the functional state of the elements of the devices, networks and telecommunications Industry 4.0]. St. Petersburg: Polytechnic Press. 121 p. (In Russian)
6. Vasiliev N. V., Zabrodin O. V., Yashin A. I. (2018). Avtomatizirovannyj programmnyj kompleks ocenki kachestva obsluzhivaniya v telekommunikacionnoj seti [Automated software package for assessing the quality of service in a telecommunications network]. *Means of Communication Equipment*. No. 3 (143). pp. 56-61. (In Russian)
7. Vityaev E. E., Dergilev A. I., Chadaeva I. V., Vasikin Yu. Yu., Spitsina A. M., Kulakova E. V., Vishnevsky O. V., Orlov Yu. L. (2016). Poisk regul'yarny'kh kontekstny'kh signalov v genomnoj DNK [Search for regular contextual signals in genomic DNA]. Collection of scientific proceedings of the conference "Informatics-2016" (Moscow, April 24-29, 2016). Moscow. *Natsional'ny'j issledovatel'skij yadernyj universitet "MIFI"* [National Research Nuclear University "MEPhI"]. Pp. 52-62. (In Russian)
8. Matematicheskie metody dlya analiza posledovatel'nostej DNK [Mathematical methods for analyzing DNA sequences]. Moscow. Mir Publ., 1999. 349 p. (In Russian)
9. Ulyanov M. V., Smetanin Yu. G. (2017). Ob odnom kharakteristicheskom funktsional'e slov nad konechny'm alfavitom [On one characteristic functional of words over a finite alphabet]. *Information technologies*. Vol. 23. No. 5. Pp. 333-341. (In Russian)
10. Sidyakin I., Ulyanov M. V. (2018). E'ffektivny'j po vremeni algoritm rascheta obobshhennoj e'ntropii dvumerny'kh slov metodom skol'zyashhego okna [Time-efficient algorithm for calculating the generalized entropy of two-dimensional words by the sliding window method]. *Sovremennye informatsionny'e tekhnologii i IT-obrazovanie* [Modern information technologies and IT education]. Vol. 14. No. 3. Pp. 560-566. (In Russian)
11. Petrushin V. N., Ulyanov M. V. (2012). Bikriterial'nyj metod postroeniya gistogramm [Bicriteria method of constructing histograms]. *Informatsionnye tekhnologii i vychislitelnye sistemy*. No. 4. Pp. 22-31. (In Russian)
12. Abramov O. V. (2017). Planirovaniye profilakticheskikh korektsiy parametrov tekhnicheskikh ustrojstv i sistem [Planning of preventive corrections of parameters of technical devices and systems]. *Informatics and control systems*. No. 3 (53). Pp. 55-66.
13. Grobust P. (2008). Sposoby ocenok skhodstva vremennykh ryadov [Methods of evaluations of the similarity of time series]. *Nauchnye trudy Mezhdunarodnoj NTK "Teoriya veroyatnostej, sluchajnye processy, matematicheskaya statistika i prilozheniya"* [Proceedings of the International NTK "Theory of probability, stochastic processes, mathematical statistics and applications", Minsk. BGU, 15-19 September 2008]. Minsk. Belarusian state University. Pp. 23-24. (In Russian)
14. Smetanin Yu. G., Ulyanov M. V., Pestova A. S. (2016). E'ntropijny'j podkhod k postroeniyu mery` simvol'nogo raznoobraziya i ego primeneniye k klasterizatsii genomov rastenij [Entropic approach to constructing a measure of symbolic diversity and its application to clustering of plant genomes]. *Mathematical biology and bioinformatics*. Vol. 11. No. 1. Pp. 114-126. (In Russian)
15. Lind D., Marcus B. (1995). An introduction to symbolic dynamics and coding. Cambridge, UK: Cambridge University Press. 495 p.
16. Vinogradenko A. M. (2020). Metodologiya intellektual'nogo kontrolya tekhnicheskogo sostoyaniya avtomatizirovannoj sistemy svyazi special'nogo naznacheniya [Methodology of intelligent control of the technical condition of an automated special-purpose communication system]. St. Petersburg: Naukoemkie tekhnologii Publ., 180 p. (In Russian)
17. Podinovskiy V. V. (2019). Idei i metody teorii vazhnosti kriteriev v mnogokriterial'nykh zadachah prinyatiya reshenij [Ideas and methods of the theory of the importance of criteria in multi-criteria decision-making problems]. Moscow: Nauka Publ. 103 p. (In Russian)
18. Holleczeck T. (2008). Statistical Analysis of IP Performance Metrics in International Research and Educational Networks. Nuremberg. Pp. 105-114.
19. Korolev V. Yu. (2007). EM-algoritm, ego modifikatsii i ih primeneniye k zadache razdeleniya smesey veroyatnostnykh raspredelenij [EM-algorithm, its modifications and their application to the problem of separation of mixtures of probability distributions]. Moscow. IPIRAN Publ. 94 p. (in Rus).
20. Allakin V. V. (2021). Analysis of methods for estimating time series by the monitoring server of a public information and telecommunications network. *Means of Communication Equipment*. No. 2 (154). Pp. 62-82. (In Russian)
21. Allakin V. V., Budko N. P., Vasiliev N. V. (2021). A general approach to the construction of advanced monitoring systems for distributed information and telecommunications networks. *Systems of Control, Communication and Security*. No. 3. Pp. 125-227. DOI: 10.24412/2410-9916-2021-4-125-227. (In Russian)

## INFORMATION ABOUT AUTHOR:

**Vladimir V. Allakin**, postgraduate student, Federal State Budgetary Educational Institution of Higher Education "Admiral S. O. Makarov State University of the Sea and River Fleet", St. Petersburg, Russia, vladimir@duduh.ru

**For citation:** Allakin V.V. The method of preventive identification of the state of monitoring objects based on the symbolic representation of time series of their metrics. *H&ES Research*. 2021. Vol. 13. No. 5. Pp. 13-28. doi: 10.36724/2409-5419-2021-13-5-13-28 (In Rus)





doi: 10.36724/2409-5419-2021-13-5-29-37

# МЕТОДИКА АНАЛИЗА ПОСТРОЕНИЯ СТРУКТУРНОГО РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ПРОТИВНИКА

**БАГРЕЦОВ**

**Сергей Алексеевич<sup>1</sup>**

**ГАЛКИН**

**Илья Андреевич<sup>2</sup>**

**АЧКАСОВ**

**Николай Борисович<sup>3</sup>**

**ИВАНОВ**

**Денис Александрович<sup>4</sup>**

## АННОТАЦИЯ

**Введение:** рассматриваются проблемы построения информационно-телекоммуникационной сети с позиции фрагментарного развития на основе методики реализации структурно-топологических принципов обеспечения живучести при построении информационно-телекоммуникационной сети. Информационно-телекоммуникационные сети относятся к классу больших систем. Она не могут быть созданы за короткое время и предполагают фрагментарное (эволюционное) развитие. Поэтому одни ее элементы могут эксплуатироваться, другие - проектироваться, а третьи – исследоваться. По этой причине методология должна включать не только методы синтеза, методы алгоритмической и параметрической оптимизации (системное проектирование), но и методы инженерного проектирования (реализации результатов синтеза). **Цель исследования:** с этой целью предлагается методика реализации структурно-топологических принципов обеспечения живучести при построении информационно-телекоммуникационной сети, включающая методику построения структурно резервированной информационно-телекоммуникационной сети, реализующая интеграционный – триадный принцип ее построения, алгоритм построения опорного варианта структуры сети и алгоритм ее корреляции с учетом применения противником средств и методов противодействия. **Методы:** предложенная методика может быть использована также для анализа сетей в условиях воздействия противника, когда необходима модернизация информационно-телекоммуникационной сети с преобразованием сети. **Результаты:** результаты свидетельствуют об адекватности и эффективности применения методики для решения задачи построения сети при ее проектировании, а также для анализа сетей в условиях воздействия противника, когда необходима модернизация информационно-телекоммуникационной сети с преобразованием сети. В результате вычисления порядковой функции графа, отражающего иерархическую структуру узлов связи информационно-телекоммуникационной сети, получено их иерархическое распределение, определяющее опорную структуру системы. В рамках этой структуры ищется ее рациональный вариант. Таким образом, для оценки адекватности и эффективности предложенной сети необходимо сравнить альтернативные варианты построения сети. Информационно-телекоммуникационная сеть, полученная в результате применения предложенной методики построения, по своим характеристикам соответствует поставленным целям, т. е. соответствует сети, являющейся результатом многолетнего опыта и неоднократных доработок, имеющих целью наиболее эффективно осуществлять взаимный обмен информацией в соответствии с условиями воздействия противника, **Обсуждение:** полученная сеть лучше, так как более устойчива при воздействии противника, а существующая сеть удовлетворяет условиям, которые существуют в данный конкретный промежуток времени, и при воздействии противника ухудшает свои показатели.

## Сведения об авторах:

<sup>1</sup> д.т.н., профессор в Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, s.bagretsov@mail.ru

<sup>2</sup> к.т.н., преподаватель в Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, ilia\_galkin@mail.ru

<sup>3</sup> д.в.н., профессор в Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, nik.achkisov@mail.ru

<sup>4</sup> к.т.н., преподаватель филиала Военного Учебного Научного центра Военно-воздушных Сил "Военно-воздушная Академия" имени профессора Н.Е. Жуковского и Ю.А. Гагарина в г. Челябинске, г. Челябинск, Россия, prosto\_deniss@mail.ru

**КЛЮЧЕВЫЕ СЛОВА:** информационно-телекоммуникационная сеть, информационный поток, опорная структура сети, живучесть

**Для цитирования:** Багрецов С.А., Галкин И.А., Ачкасов Н.Б., Иванов Д.А. Методика анализа построения структурного резервирования информационно-телекоммуникационной сети в условиях воздействия противника // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 29-37. doi: 10.36724/2409-5419-2021-13-5-29-37

**Введение**

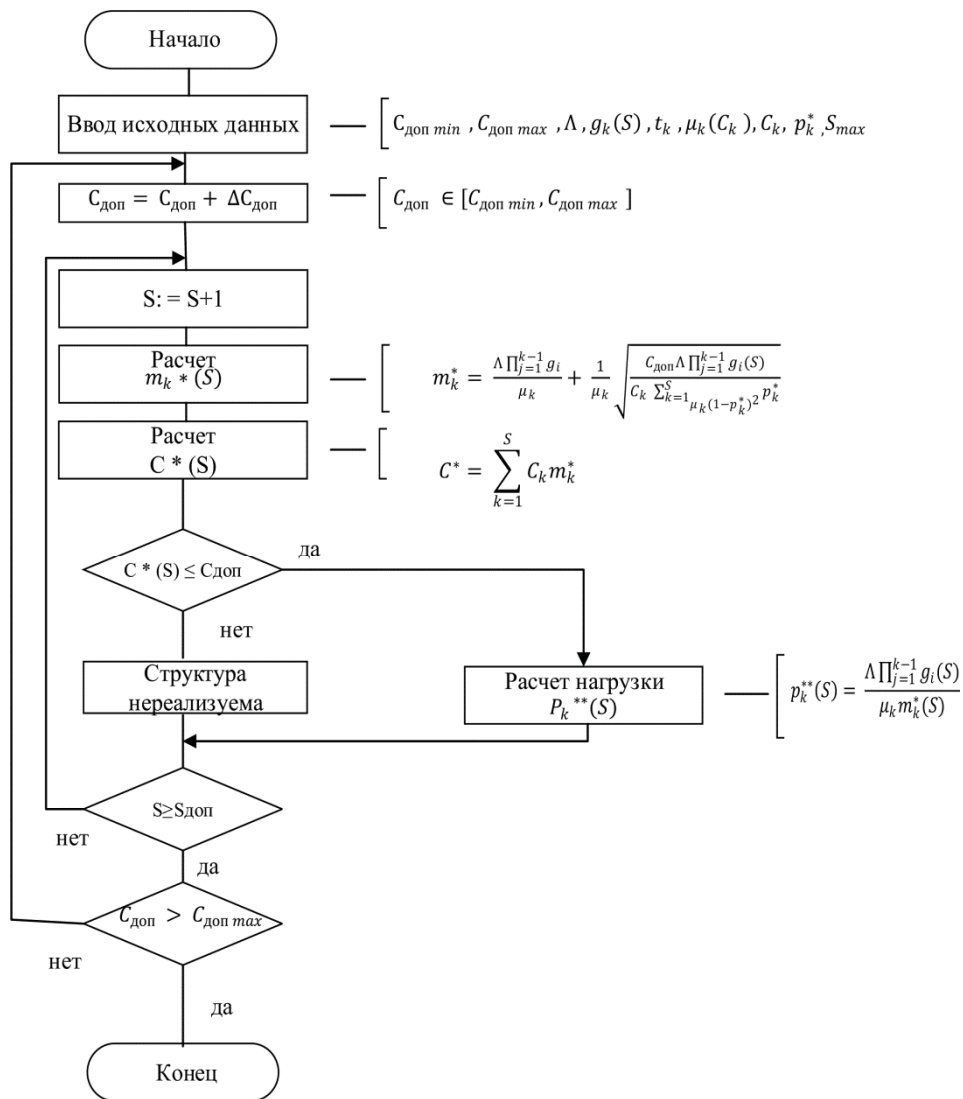
Информационно-телекоммуникационные сети (ИТКС) относятся к классу больших систем. Она не могут быть созданы за короткое время и предполагают фрагментарное (эволюционное) развитие. Поэтому одни ее элементы могут эксплуатироваться, другие – проектироваться, а третьи – исследоваться. По этой причине методология должна включать не только методы синтеза, методы алгоритмической и параметрической оптимизации (системное проектирование), но и методы инженерного проектирования (реализации результатов синтеза).

С этой целью предлагается методика реализации структурно-топологических принципов обеспечения живучести при построении ИТКС, включающая методику построения структурно резервированной ИТКС, реализующая интеграционный – триадный принцип ее построения, алгоритм построения опорного варианта структуры сети и алгоритм ее корреляции с учетом применения противником средств и методов противодействия.

В результате вычисления порядковой функции графа, отражающего иерархическую структуру узлов связи (УС) ИТКС, получено их иерархическое распределение, определяющее опорную структуру системы. В рамках этой структуры ищется ее рациональный вариант.

Для синтеза опорного варианта структуры ИТКС и разработки алгоритма ее корреляции с учетом применения противником средств и методов противодействия в методике используются следующие критерии минимизации: количества УС; среднего времени решения оперативных задач УС в ИТКС; показателей равномерности загрузки между УС; общей стоимости содержания структуры ИТКС.

Расчетные выражения и блок-схемы определения рациональных (опорных) вариантов структуры ИТКС по минимуму времени обработки информации на УС и минимуму стоимости представлены на рисунках 1 и 2. Опорный вариант ИТКС является основой для принятия решения экспертом о целесообразности или нецелесообразности дальнейшего изменения структуры ИТКС [1, 2].



**Рис. 1.** Блок-схема определения рациональных вариантов структуры ИТКС по минимуму времени обработки информации на УС

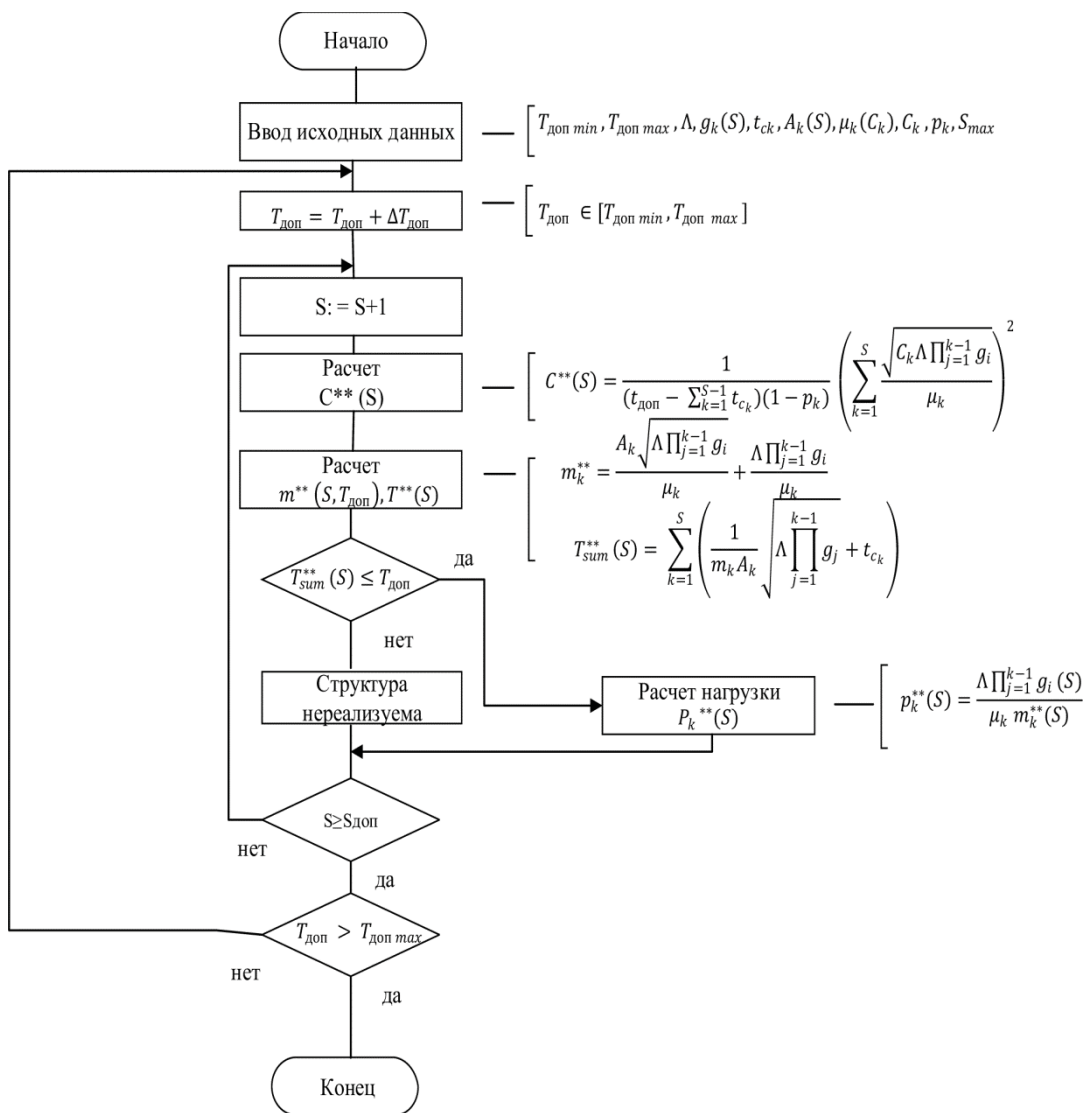


Рис. 2. Блок-схема определения рациональных вариантов структуры ИТКС по минимуму стоимости

Для того чтобы обеспечить объективность в сравнении результатов синтеза, приняты единые исходные данные по возможностям УС: потоковой нагрузке, количеству информационных направлений, стоимости единицы техники связи. С учетом специфики ведения технической разведки и воздействия, а также специфики функционирования ИТКС по этим этапам решались задачи:

- управления маршрутами передачи сообщений в ИТКС;
- поиска опорного варианта ИТКС;
- поиска зоны регулируемого равновесия взаимного обмена информацией в каналах связи [3, 5].

Для проверки адекватности и эффективности предложенной методики проведен вычислительный эксперимент. Был определен опорный вариант ИТКС. В качестве исходных данных для синтеза были выбраны характеристики реальной функционирующей сети.

По этим данным проведен синтез сети в предположении, что проектируется новая, ранее неизвестная система управления.

Цель эксперимента заключается в том, чтобы по результатам сравнения реальной функционирующей сети и сети, синтезированной по предложенной методике, оценить адекватность и эффективность использования данной методики для обоснования опорного варианта структурно-резервированной ИТКС с учетом применения противником средств и методов противодействия.

Для достижения цели эксперимента решались следующие задачи:

- оценка исходных данных, необходимых для решения задачи построения ИТКС;
- построение опорного варианта ИТКС по предложенной методике;
- сравнение синтезированной и существующей сетей.

По результатам вычислительного эксперимента делается вывод о возможности использования предложенного комплекса методик для построения ИТКС, перспективных систем управления уже на ранних этапах проектирования.

### Построение сети

В соответствии с условиями решения задачи построения сети считаются известными следующие исходные данные: объем информационного обмена; ожидаемый информационный обмен в единицу времени по каждому типу трафика; среднее допустимое время существования информации и математическое ожидание времени ее передачи; ориентировочная стоимость УС и линий связи (каналов связи).

На основе опыта эксплуатации ИТКС были определены исходные данные, необходимые для решения задачи синтеза и соответствующие существующей ИТКС.

В множество  $X = \{x_1 \dots x_n\}$  элементов сети, необходимых для решений общей задачи ИТКС, вошли следующие задачи управления:

- $x_1$  – главный центр связи 1 уровня (ГЦС 1);
- $x_2$  – центр связи 2 уровня (ЦС 2);
- $\{x_3 \dots x_{12}\}$  – узлы связи 3 уровня (УС 3);
- $\{x_{13} \dots x_{17}\}$  – узлы связи 4 уровня (УС 4);
- $\{x_{18} \dots x_{31}\}$  – узлы связи 5 уровня (УС 5).

Исходные данные по ожидаемой интенсивности информационного обмена, математическому ожиданию времени информационного обмена и среднему допустимому времени передачи информации для каждого типа трафика представлены в таблице 1.

Таблица 1

Исходные данные по ожидаемой интенсивности информационного обмена, математическому ожиданию времени информационного обмена и среднему допустимому времени передачи информации

Тип (γ) трафика	Интенсивность, 1/ч	Время передачи, ч	( $t_{доп.1}$ ), ч	Тип (γ) трафика	Интенсивность, 1/ч	Время передачи, ч	( $t_{доп.1}$ ), ч
x1		0,25	0,3	x 17	0,3	3,3	0,25
x 2	4	0,25	0,2	x 18	0,2	5	0,25
x 3	1	1	0,4	x 19	0,2	5	0,08
x 4	0,6	1,7	0,4	x 20	0,2	5	0,5
x 5	0,6	1,7	0,19	x 21	0,2	5	0,4
x 6	0,6	1,7	0,88	x 22	0,2	5	0,2
x 7	0,6	1,7	0,5	x 23	0,2	5	0,2
x 8	0,6	1,7	0,33	x 24	0,2	5	0,33
x 9	0,6	1,7	0,25	x 25	0,2	5	0,33
x 10	0,7	1,4	0,4	x 26	0,2	5	0,3
x 11	1	1	0,08	x 27	0,2	5	0,7
x 12	0,5	2	0,5	x 28	0,2	5	0,5
x 13	0,4	2,5	0,25	x 29	0,2	5	0,5
x 14	0,5	2	0,3	x 30	0,2	5	0,08
x 15	0,5	2	0,38	x 31	0,2	5	1,0
x 16	0,3	3,3	0,33				

Допустимая стоимость синтезируемой структуры ИТКС была выбрана в соответствии с уровнем суммарных затрат на создание существующей структуры ИТКС. Ограничения по вероятности правильного и своевременного информационного обмена по загруженности и равномерности загрузки УС были приняты соответственно:  $P_{доп} > 0,85$ ;  $K_3 = [0,3; 0,75]$ ,  $K_p = [0,1; 0,15]$ . В соответствии с предложенной методикой синтеза ИТКС были выполнены следующие этапы синтеза:

- оценка взаимного обмена информацией;
- выделение сильно связанного взаимного обмена информацией;
- вертикальная структуризация взаимного обмена информацией;
- определение опорного варианта структуры ИТКС;
- определение рационального варианта структуры ИТКС.

### Оценка взаимных связей между УС в ИТКС

Связи между УС определялись по следующим признакам: время начала и окончания обмена информацией; место обмена информацией; причинно-следственные связи; использование входных и выходных данных; семантические связи.

Оценка выбранных признаков была проведена на основе анализа трафика в существующей сети связи. Расчет меры близости взаимного обмена информацией производился на основе взвешенного коэффициента Танимото-Роджерса.

По результатам расчета составлена матрица мер близости (рис. 3) в соответствии с графом взаимной связи ИТКС (рис. 4), в котором цифрами показана важность линий связи в информационном обмене сети.

	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12	x13	x14	x15	x16	x17	x18	x19	x20	x21	x22	x23	x24	x25	x26	x27	x28	x29	x30	x31
x1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x2	0	1	0,5	0,5	0,5	0,5	1	0,5	0,5	0,5	0,5	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x8	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x9	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x10	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x11	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x12	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x13	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0,5	0,5	0,5	0,5	0	0	0	0	0	0	0	0	0	0	
x14	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
x15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0,5	0,5	0,5	0,5	0	0	0	0	0	
x16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0,5	0,5	0,5	0,5	0,5	
x17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0,5	0,5	0,5	
x18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
x19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	
x20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	
x21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	
x22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
x23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	
x24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	
x25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	
x26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	
x27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	
x28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	
x29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
x30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
x31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Рис. 3. Матрица мер близости взаимного обмена информацией







## Заключение

Таким образом, для оценки адекватности и эффективности предложенной сети необходимо сравнить альтернативные варианты построения сети. Цель – наиболее эффективно решать поставленные задачи в соответствии с условиями воздействия противника, т. е. необходимо выявить сходства и отличия полученной и существующей сетей, проанализировать причины и последствия выявленных различий.

Сравнение сетей проводилось по показателям, характеризующим:

- глубину иерархии, число УС и линий связи;
- количество и характер связей сети;
- правильное и своевременное обеспечение взаимного обмена информацией.

Обе сети являются многоуровневыми иерархическими. Различия в количестве и составе УС обусловлены характером взаимного обмена информацией между УС ИТКС. Различия в количестве УС вызваны тем, что задача оперативно-го обмена информацией, решавшаяся в существующей сети ГЦС (1-й уровень иерархии), в полученной сети решается во втором (ЦС 1). Данное перераспределение задач объясняется тесной взаимосвязью существующих задач и необходимостью их совместного (параллельного) решения. Поэтому полученная в результате синтеза структура ИТКС фактически отражает сложившуюся и свидетельствует о необходимости ее учета при проектировании УС.

Третий и четвертый уровень иерархии УС полученной сети практически повторяют построение соответствующих УС в существующей ИТКС, за исключением дополнительных точек доступа.

Выявленные отличия сетей в ряде случаев обусловлены влиянием субъективных факторов, не учитываемых в предлагаемой методике. К таким факторам относятся исторически сложившаяся структура аналогичных ИТКС, стремление к однообразию и др.

ИТКС, полученная в результате применения предложенной методики построения, по своим характеристикам соответствует поставленным целям, т. е. соответствует сети, являющейся результатом многолетнего опыта и неоднократных доработок, имеющих целью наиболее эффективно осуществлять взаимный обмен информацией в соответствии с условиями воздействия противника.

Полученная сеть лучше, так как более устойчива при воздействии противника, а существующая сеть удовлетворяет условиям, которые существуют в данный конкретный промежуток времени, и при воздействии противника ухудшает свои показатели.

Результаты эксперимента свидетельствуют об адекватности и эффективности применения предложенной методики для решения задачи построения сети при ее проектировании.

Предложенная методика может быть использована также для анализа сетей в условиях воздействия противника, когда необходима модернизация ИТКС с преобразованием сети.

## Литература

1. Баранов В.В., Максимова Е.А., Лаута О.С. Анализ модели информационного обеспечения процессов и систем при реализации многоагентного интеллектуального взаимодействия // Приборы и системы. Управление, контроль, диагностика. 2019. № 4. С. 32-41.
2. Власенко М.А., Иванов Д.А., Кузнецов С.И., Лаута О.С. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 167-171.
3. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П., Муртазин И.Р. Методика прогнозирования воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть В сборнике: Региональная информатика и информационная безопасность. 2017. С. 109-111.
4. Коцыняк М.А., Иванов Д.А. Обеспечение безопасности управления роботизированных систем от воздействия таргетированных кибернетических атак В книге: Нейрокомпьютеры и их применение. Тезисы докладов. 2018. С. 108-А.
5. Коцыняк М.А., Лаута О.С., Иванов Д.А., Лукина О.М. Модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 3-4 (129-130). С. 58-65.
6. Лаута О.С., Иванов Д.А., Нечепуренко А.П., Власенко М.А. Методика синтеза системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 124-129.
7. Гудков М.А., Лаута О.С., Иванов Д.А., Соловьев Д.В. Применение методов искусственного интеллекта в задачах обеспечения информационной безопасности. Современные информационные технологии. 2018. С. 162.
8. Лаута О.С., Коцыняк М.А., Иванов Д.А., Суетин А.И. Методика прогнозирования воздействия компьютерных атак на информационно-телекоммуникационную сеть В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 115-123.
9. Иванов Д.А., Мамай А.В., Стицын О.Л., Карасев И.В. Подход к обоснованию структуры воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 2 (34). С. 107-110.
10. Коцыняк М.А., Лаута О.С., Иванов Д.А., Кузнецов С.И. Применение международного стандарта iso/iec 27032:2012, регламентирующего политическую и военную деятельность в киберпространстве В сборнике: Современные информационные технологии. Теория и практика. Материалы IV Всероссийской научно-практической конференции. Отв. ред. Т.О. Петрова. 2018. С. 192-196.
11. Кузнецов С.И., Иванов Д.А., Власенко М.А., Латушко Н.А. Вероятностно-временные характеристики атак на роботизированные системы В сборнике: Региональная информатика и информационная безопасность. 2017. С. 117-118.
12. Багрецев С.А., Лаута О.С., Шукин А.В., Иванов Д.А. Методика обоснования эффективной групповой деятельности операторов с двухуровневой структурой организации Известия Тульского государственного университета. Технические науки. 2021. № 6. С. 20-29.

13. Багрецов С.А., Лаута О.С., Михаил И.И., Иванов Д.А. Методика обоснования рационального количества резервных каналов связи в информационно-телекоммуникационной сети Электро-связь. 2020. № 8. С. 31-38.

14. Евстигнеев А.С., Зорин К.М., Карпов М.А., Костырев А.Л., Максимов Р.В., Орлов Е.В., Павловский А.В. Способ мониторинга безопасности автоматизированных систем / Патент на изобретение RU 2355024 С2, 10.05.2009. Заявка № 2007105319/09 от 12.02.2007.

15. Neural networks for control/ Miller W.T., Sutton R.S., Werbos P.J., Eds., The MIT Press, 1990.8. ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».

16. Коцыняк М.А., Карпов М.А., Лаута О.С., Дементьев В.Е. // Управление системой обеспечения безопасности информационно-телекоммуникационной сетью на основе алгоритмов функционирования искусственной нейронной сети». Известия Тульского государственного университета. Технические науки. 2020. № 4. С. 3-10.

17. Тали Д.И., Финько О.А. Криптографический рекурсивный контроль целостности метаданных электронных документов. Часть 4. Оценка защищенности Вопросы кибербезопасности. 2021. № 2 (42). С. 37-50.

18. Багрецов С.А., Лаута О.С., Михаил И.И., Михайлец А.Н., Бойко Д.А. Повышение устойчивости информационно-телекоммуникационной сети в условиях воздействия противника I-methods. 2020. Т. 12. № 2. С. 1-13.

19. Багрецов С.А., Бударин Э.А., Лаута О.С., Митрофанов М.В. Методика повышения устойчивости иткс в условиях воздействия противника на основе определения опорного варианта Электросвязь. 2020. № 9. С. 64-68.

20. Багрецов С.А., Ачкасов Н.Б., Лаута О.С., Васюков Д.Ю. Методика обоснования рационального маршрута передачи информации в иткс при комплексном воздействии противника Труды Научно-исследовательского института радио. 2020. № 3. С. 67-80.

## METHODOLOGY FOR ANALYZING THE CONSTRUCTION OF STRUCTURAL REDUNDANCY OF AN INFORMATION AND TELECOMMUNICATIONS NETWORK UNDER THE INFLUENCE OF THE ENEMY

**SERGEY A. BAGRETSOV,**

St-Petersburg, Russia, s.bagretsov@mail.ru

**ILYA A. GALKIN,**

St-Petersburg, Russia, ilia\_galkin@mail.ru

**NIKOLAY B. ACHKASOV,**

St-Petersburg, Russia, nik.achkisov@mail.ru

**DENIS A. IVANOV,**

Chelyabinsk, Russia, prosto\_deniss@mail.ru

### ABSTRACT

**Introduction:** the problems of building an information and telecommunications network are considered from the position of fragmentary development based on the methodology of implementing structural and topological principles of ensuring survivability in the construction of an information and telecommunications network. Information and telecommunication networks belong to the class of large systems. They cannot be created in a short time and assume fragmentary (evolutionary) development. Therefore, some of its elements can be exploited, others can be designed, and others can be investigated. For this reason, the methodology should include not only synthesis methods, algorithmic and parametric optimization methods (system design), but also engineering design methods (implementation of synthesis results). **Purpose:** a methodology is proposed for the implementation of structural and topological principles of ensuring survivability in the construction of an information and telecommunications network, including a methodology for constructing a structurally redundant information and telecommunications network, implementing the integration – triad principle of its construction, an algorithm for constructing a reference variant of the network structure and an algorithm for its correlation, taking into account the use of means and methods of counteraction by the enemy. The questions of the structural and mathematical definition of the methodology for constructing a structurally redundant information and telecommunications network that implements the integration – triad principle of its construction, the algorithm for constructing a reference version of the network structure and the algorithm for

**KEYWORDS:** information and telecommunication network; information flow; network support structure; survivability.

its correlation, considering the use of means and methods of counteraction by the enemy, are presented. **Methods:** the proposed methodology can also be used to analyze networks under the influence of the enemy, when it is necessary to modernize the information and telecommunications network with network transformation. **Results:** the results indicate the adequacy and effectiveness of the methodology for solving the problem of building a network in its design, as well as for analyzing networks under the influence of the enemy, when it is necessary to modernize the information and telecommunications network with the transformation of the network. As a result of calculating the ordinal function of the graph reflecting the hierarchical structure of communication nodes of the information and telecommunications network, their hierarchical distribution determining the reference structure of the system is obtained. Within the framework of this structure, its rational variant is being sought. Thus, to assess the adequacy and effectiveness of the proposed network, it is necessary to compare alternative options for building a network. The information and telecommunication network obtained as a result of the application of the proposed construction methodology corresponds in its characteristics to the set goals, i.e. corresponds to a network that is the result of many years of experience and repeated improvements aimed at the most effective mutual exchange of information in accordance with the conditions of the enemy's influence. **Discussion:** the resulting network is better, since it is more stable when exposed to the enemy, and the existing network satisfies the conditions that exist in this particular period of time, and when exposed to the enemy worsens its performance.



## REFERENCES

1. Baranov V.V., Maksimova E.A., Laut O.S. (2019). Analysis of the model of information support of processes and systems in the implementation of multi-agent intelligent interaction. *Devices and systems. Management, control, diagnostics*. No. 4. pp. 32-41. (In Russian)
2. Vlasenko M.A., Ivanov D.A., Kuznetsov S.I., Laut O.S. (2018). In the collection: Actual problems of infotelecommunications in science and education (APINO 2018). VII International Scientific-technical and scientific-methodical conference. *Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky*. Pp. 167-171. (In Russian)
3. Kotsynyak M.A., Ivanov D.A., Laut O.S., Nechepurenko A.P., Murtazin I.R. (2017). Methodology for predicting the impact of a targeted cybernetic attack on an information and telecommunications network. *In the collection: Regional Informatics and information security*. Pp. 109-111. (In Russian)
4. Kotsynyak M.A., Ivanov D.A. (2018). Ensuring the security of control of robotic systems from the effects of targeted cybernetic attacks In the book: Neurocomputers and their application. Abstracts of reports. P. 108-A. (In Russian)
5. Kotsynyak M.A., Laut O.S., Ivanov D.A., Lukina O.M. (2019). A model of the impact of a targeted cybernetic attack on the information and telecommunications network Issues of defense technology. *Series 16: Technical means of countering terrorism*. No. 3-4 (129-130). pp. 58-65. (In Russian)
6. Laut O.S., Ivanov D.A., Nechepurenko A.P., Vlasenko M.A. (2018). Methods of synthesis of the information and telecommunication network protection system in the conditions of information confrontation *In the collection: Radar, navigation, communication. Proceedings of the XXIV International Scientific and Technical Conference*. In 5 volumes. Pp. 124-129. (In Russian)
7. Gudkov M.A., Laut O.S., Ivanov D.A., Soloviev D.V. (2018).. Application of artificial intelligence methods in information security tasks. *Modern information technologies*. P. 162. (In Russian)
8. Laut O.S., Kotsynyak M.A., Ivanov D.A., Suetin A.I. (2018). Methods of predicting the impact of computer attacks on the information and telecommunications network In the collection: Radar, navigation, communication. *Proceedings of the XXIV International Scientific and Technical Conference*. In 5 volumes. Pp. 115-123. (In Russian)
9. Ivanov D.A., Mamai A.V., Spitsyn O.L., Karasev I.V. (2019). Approach to substantiating the structure of the impact of a targeted cybernetic attack on the information and telecommunications network *Information technologies and systems: management, economics, transport, law*. No. 2 (34). pp. 107-110. (In Russian)
10. Kotsynyak M.A., Laut O.S., Ivanov D.A., Kuznetsov S.I. (2018). Application of the international standard iso/iec 27032:2012 regulating political and military activities in cyberspace *In the collection: Modern Information technologies. Theory and practice. Materials of the IV All-Russian Scientific and Practical Conference*. Ed. by T.O. Petrov. Pp. 192-196. (In Russian)
11. Kuznetsov S.I., Ivanov D.A., Vlasenko M.A., Latushko N.A. (2017). Probabilistic-temporal characteristics of attacks on robotic systems. *In the collection: Regional Informatics and information security*. Pp. 117-118.
12. Bagretsev S.A., Laut O.S., Shchukin A.V., Ivanov D.A. (2021). Methodology for substantiating the effective group activity of operators with a two-level structure of the organization of the News of Tula State University. *Technical sciences*. No. 6. pp. 20-29. (In Russian)
13. Bagretsov S.A., Laut O.S., Mikhail I.I., Ivanov D.A. (2020). Methodology for substantiating the rational number of backup communication channels in the Telecommunication information network. No. 8. Pp. 31-38. (In Russian)
14. Evstigneev A.S., Zorin K.M., Karpov M.A., Kostyrev A.L., Maksimov R.V., Orlov E.V., Pavlovsky A.V. Method of monitoring the safety of automated systems / Patent for invention RU 2355024 C2, 05/10/2009. Application No. 2007105319/09 dated 12.02.2007. (In Russian)
15. Miller W.T., Sutton R.S., Werbos P.J. Neural networks for control/, Eds., The MIT Press, 1990.8. GOST R 50922-2006. "Information protection. Basic terms and definitions".
16. Kotsynyak M.A., Karpov M.A., Laut O.S., Dementiev V.E. (2020). Management of the information and telecommunication network security system based on artificial neural network functioning algorithms". *Proceedings of Tula State University. Technical sciences*. No. 4. Pp. 3-10. (In Russian)
17. Tali D.I., Finko O.A. (2021). Cryptographic recursive control of the integrity of metadata of electronic documents. Part 4. *Security Assessment Cybersecurity issues*. No. 2 (42). Pp. 37-50.
18. Bagretsov S.A., Laut O.S., Mikhail I.I., Mikhailets A.N., Boyko D.A. (2020). Increasing the stability of the information and telecommunications network under the influence of the enemy. *I-methods*. Vol. 12. No. 2. Pp. 1-13. (In Russian)
19. Bagretsov S.A., Budarin E.A., Laut O.S., Mitrofanov M.V. (2020). Methodology for increasing the stability of ITCS in the conditions of enemy influence based on the definition of the reference variant of Telecommunication. No. 9. Pp. 64-68. (In Russian)
20. Bagretsov S.A., Achkasov N.B., Laut O.S., Vasyukov D.Yu. (2020). Methodology for substantiating the rational route of information transmission to ITCS under the complex influence of the enemy *Proceedings of the Radio Research Institute*. No. 3. Pp. 67-80 (In Russian)

## INFORMATION ABOUT AUTHORS:

**Sergey A. Bagretsov**, PhD, Full Professor, Professor of the military Academy of Communications

**Ilya A. Galkin**, PhD, Lecturer of the military Academy of Communications

**Nikolay B. Achkasov**, PhD, Professor of the military Academy of Communications

**Denis A. Ivanov**, PhD, Lecturer of the branch of the Military Training Scientific Center of the Air Force "Air Force Academy"

---

**For citation:** Bagretsov S.A., Galkin I.A., Achkasov N.B., Ivanov D.A. Methodology for analyzing the construction of structural redundancy of an information and telecommunications network under the influence of the enemy. H&ES Reserch. 2021. Vol. 13. No. No 5. P. 29-37. doi: 10.36724/2409-5419-2021-13-5-29-37 (In Rus)

doi: 10.36724/2409-5419-2021-13-5-38-56

## МЕТОДИКА СИНТЕЗА ПОДСИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОГО МОНИТОРИНГА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СИТУАЦИОННОГО ЦЕНТРА

**БУДКО**

**Никита Павлович<sup>1</sup>**

### АННОТАЦИЯ

**Введение:** в соответствии с задачей по формированию системы распределенных ситуационных центров органов государственной власти требуется осуществить сопряжение разнородных сегментов информационно-телекоммуникационных сетей ведомства в территориально-распределенную инфраструктуру с построением на ней подсистемы мониторинга состояния ее элементов. **Цель исследования:** на основе использования базовых понятий методов структурного синтеза, структурного анализа сетевых инфраструктур, а также процедур параметрического синтеза, разработать методику синтеза подсистемы мониторинга нового поколения, базирующуюся на интеллектуальных методах идентификации состояния сети. **Результаты:** структуризация контролируемого пространства терминами "зона мониторинга", "критически важный элемент", "классы состояния" составляют основу новых методов интеллектуального мониторинга, являющихся "нечувствительными" к свойствам постоянного эволюционирования сетевых инфраструктур. Предложенная методика синтеза подсистемы интеллектуального мониторинга состоит из последовательно выполняемых этапов структурного синтеза, параметрического синтеза и структурного анализа сети. **Практическая значимость:** последовательно проведенные этапы методики с использованием процедур измерения графовых расстояний и модифицированного алгоритма  $k$ -средних, позволяют не только идентифицировать вид состояния сети, но и обоснованно, с использованием инструментальных методов расчета, представить в интересах системы поддержки принятия решения наборы приемлемых значений основных параметров и вероятно-временных характеристик подсистемы мониторинга для последующей переконфигурации сети и недопущения её перехода в неработоспособное состояние. **Обсуждение:** предложенная в исследовании модификация алгоритма  $k$ -средних отличается тем, что в классическом алгоритме работа ведется над точками Евклидова пространства, а в предлагаемой методике речь идет о графовом пространстве с метриками в виде графовых расстояний, при этом в качестве исходных данных для классификации в алгоритме  $k$ -средних используются облака данных как неупорядоченные наборы данных, не привязанные к какой-либо из шкал измерений, а в предлагаемом алгоритме облако данных представлено множеством графов в заданном топологическом пространстве метрик графов, описывающих состояния сети во времени.

### Сведения об авторе:

<sup>1</sup> аспирант, Федеральное государственное бюджетное образовательное учреждение высшего образования "Государственный университет морского и речного флота имени адмирала С.О. Макарова".  
г. Санкт-Петербург, Россия,  
budko62@mail.ru

**КЛЮЧЕВЫЕ СЛОВА:** алгоритм  $k$ -средних, идентификация вида состояния сети, медианный граф, подсистема мониторинга, этап параметрического синтеза, этап структурного анализа, этап структурного синтеза.

**Для цитирования:** Будко Н.П. Методика синтеза подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети ситуационного центра // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 38-56. doi: 10.36724/2409-5419-2021-13-5-38-56

## Введение

Возрастающая роль ситуационных центров (СЦ)<sup>1</sup> в вопросах создания и развития экономики нового уклада в России на основе современных информационных технологий сегодня общепризнанный факт, закрепленный многими руководящими документами уровня Президента Российской Федерации (РФ) и Правительства РФ [1]. Тем не менее, на данный момент только половина федеральных органов исполнительной власти (ОИВ), а также федеральных служб и агентств имеют полноценные СЦ, создаваемые в соответствии с Указом Президента РФ № 648 от 25.07.2013 г. «О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия». Иерархически структура сети СЦ ОИВ включает в себя:

высший уровень – СЦ Президента РФ, СЦ Правительства РФ, СЦ Администрации Президента РФ, СЦ Совета безопасности РФ;

второй уровень – СЦ полномочных представителей Президента РФ в федеральных округах, СЦ руководителей министерств и ведомств;

третий уровень – СЦ глав субъектов РФ, СЦ корпораций и предприятий [1].

В тех ОИВ, где уже приступили к созданию СЦ, программы цифровизации государственного управления могут развиваться более эффективно, обеспечивая переход от задач мониторинга к комплексному анализу, планированию и прогнозу. Для Министерства транспорта РФ задача создания СЦ не нова, поскольку в каждом федеральном агентстве Минтранса существуют инфраструктуры подобного типа, построенные на информационно-телекоммуникационных сетях (ИТКС) общего пользования (ОП), объединяющих в своем составе наземные сегменты (развернутые вдоль автомобильных и железнодорожных магистралей) со средствами сигнализации и связи при управлении автотранспортом и движением поездов (ДП), систем связи и радиотехнического обеспечения при организации системы управления воздушным движением (ВД), систем автоматизированного управления движением судов (ДС) на внутренних водных путях (ВВП) и в морских акваториях. Здесь уже проявляется иерархический принцип построения ИТКС от телекоммуникационных структур автомобильных и железных дорог, районов ВД и районных администраций бассейнов рек (озер) до единых центров управления (ЕЦУ) ДП, ЕЦУ ВД, ЕЦУ ДС.

Однако сложности создания СЦ Минтранса РФ обусловлены тем, что существующие ЕЦУ движением различных категорий транспорта являются изначально гетерогенными<sup>2</sup> даже в рамках одной системы (только международная глобальная морская система связи при бедствиях – GMDSS (англ. Global Maritime Distress and Safety System) использует сред-

ние – СЧ (МФ), высокие – ВЧ (HF), очень высокие – ОВЧ (VHF), ультравысокие – УВЧ (UHF) и сверхвысокие – СВЧ (SHF) частоты), не говоря уже о внутриведомственной или межведомственной специфике их объединения в интересах логистического взаимодействия при движении пассажиропотоков и грузоперевозок внутри РФ и при выходе на мировой уровень.

Организационно СЦ состоит из сегментов: руководства органа исполнительной власти (корпорации, предприятия); мониторинга состояния подконтрольного пространства (распределенной ИТКС); ситуационного анализа и подготовки решений (поддержки принятия решений); администрирования и эксплуатации аппаратно-программных средств (АПС) СЦ. Одним из основных сегментов СЦ является сегмент *мониторинга*, который представлен комплексом АПС, предназначенных для сбора, обработки и хранения метрик объектов мониторинга, а также выдачи оповещений о нестандартных ситуациях на подконтрольном пространстве. Ключевыми элементами сегмента мониторинга СЦ является АРМ диспетчера подсистемы мониторинга и серверы мониторинга, которые с позиции области применения и наблюдаемого пространства могут формироваться по областям применения различно, но с позиции ИТКС должны состоять из сборщика сырых данных, базы данных временных рядов и HTTP сервера, функционирующих во взаимодействии с объектами мониторинга, подсистемой оповещения и подсистемами отображения иных сегментов СЦ [3].

В соответствии с поставленной задачей по созданию СЦ Минтранса РФ требуется осуществить сопряжение разнородных сегментов ИТКС Росавтодора, Росжелдора, Росавиации, Росморречфлота и Ространснадзора в территориально-распределенную инфраструктуру с построением на ней подсистемы мониторинга состояния ее элементов. Это пересекается с общей тенденцией развития и совершенствования современных сетей связи, направленной на переход от узкопрофильных гомогенных внутриведомственных к гетерогенным межведомственным ИТКС в рамках Единого информационного пространства России. При этом важно понимать, что для эффективного управления современными ИТКС необходимо знание актуального функционального состояния сетевых элементов (в режиме реального времени), а также соединений и связей между ними (каналов связи, маршрутов, путей), что требует их полного охвата процедурами контроля и мониторинга.

Беря во внимание указанные особенности в развитии ИТКС ОП, а также высокую скорость эволюции современных систем управления, комплексов связи и их средств контроля, прошедшие этапы автоматизации (1970–1990 гг.), интеграции (1990–2010 гг.) и унификации (2010–2030 гг.), важно отметить, что мы вплотную подошли к рубежу, когда такими сложными распределенными гетерогенными структурами невозможно управлять вручную. Все это говорит о несовершенстве существующих систем контроля и научно-методического аппарата, ориентированных на использование в гомогенных сетевых структурах, а также о необходимости поиска новых технологий и подходов к построению подсистем распределенного мониторинга функционального состояния элементов современных ИТКС на основе новых методов *интеллектуального мониторинга* и контроля.

<sup>1</sup> Ситуационный центр – программно-технический комплекс, концентрирующий информацию о подконтрольном пространстве от разных источников и обеспечивающий ситуационное управление, принятие управленческих решений с широким использованием информационно-коммуникационных технологий, моделей и методов ситуационного анализа [1].

<sup>2</sup> Под гетерогенными имеются в виду, как правило, сетевые структуры, образующиеся объединением различных ведомственных сетей, имеющих разные принципы построения, сетевые технологии доставки и/или защиты информации, и/или программно-аппаратные средства [2].



Исторически сложилось, что задача синтеза территориально-распределенных ИТКС рассматривается с точки зрения трех основных этапов: структурного синтеза, параметрического синтеза и выбора (разработки) методов управления на них [2, 4-6]. В этом случае подсистемы мониторинга распределенных сетевых структур, как правило, имеют трехуровневую структуру, состоящую

из сенсорного уровня (на котором осуществляется сбор информации о функциональном состоянии сетевых элементов);

телекоммуникационного уровня (объединяющего каналы телесигнализации для передачи измерительной информации (ИИ) от сенсоров (датчиков) в центр ее обработки);

диспетчерского уровня (осуществляющего сбор ИИ, ее обработку и представление результатов обработки в удобном виде для принятия решения на управление сетью).

Учитывая, что структуры подсистем мониторинга накладываются на структуры ИТКС, используя в интересах своего телекоммуникационного уровня (каналов телесигнализации) общие каналы, может показаться, что этап синтеза подсистемы мониторинга сводится к синтезу самой сети. Однако необходимо отметить наличие существенных отличий технологий контроля и мониторинга от технологий передачи данных, а также управления современными ИТКС, что требует для распределенных гетерогенных структур решения самостоятельной задачи синтеза подсистемы мониторинга. Информационно-телекоммуникационные сети справедливо относят к системам с высокой степенью доступности и непрерывным режимом функционирования, при котором необходимо обеспечить безотказность работы узлов системы и их сервисов круглосуточно 365 дней в году. Это связано не только с тем, что каждая минута простоя для телеком-операторов и их клиентов влечет существенные финансовые и репутационные издержки. Для транспортной отрасли это сопряжено еще и с тем, что при неудовлетворительной работе ИТКС и ее критически важных приложений (сетей технологической связи) может наступить уголовная ответственность [7] водителя (машиниста, пилота, капитана) или администрации (организатора движения). При этом не только отсутствие, но и низкое качество сетевых услуг могут лечь в основу судебных претензий (при включении вопроса качества услуг в SLA-договор [8] с оператором). Таким образом, контроль функционирования сетевой инфраструктуры важен не только телеком-оператору, но и потребителю (судовладельцу, судоводителю и т. д.). Причем важно отметить, что сетевой мониторинг на сегодня является единственным объективным и надежным методом оценки параметров эффективного функционирования ИТКС, что требует разработки и совершенствования его инструментария. Так, из доклада АСФЕ [9] следует, что организации, применяющие в повседневной деятельности инструменты мониторинга и прогноза в ИТКС, снижают потери на 60 % по сравнению с организациями, их игнорирующими.

### 1. Общий подход к синтезу подсистемы интеллектуального мониторинга ИТКС ОП

Анализ этапов развития ИТКС показал экспоненциальный рост их структур, а значит и контролируемого пространства, порождаемый увеличением территориальной распределенности и неоднородности сегментов сети. При этом большая ее

степень размерности, с учетом многоуровневой структуры и гетерогенности  $\Psi(t)$ , совокупности наблюдаемых параметров (метрик), предполагает наличие такой модели системы мониторинга, которая позволит учитывать принципы построения и требования, предъявляемые к ней, что направлено на решение задачи уровня сложности  $\Psi(t) = \{Y(t), W(t)\}$ , где  $Y(t)$  и  $W(t)$  – компоненты, характеризующие топологию структуры подсистемы мониторинга и ее функциональные свойства соответственно.

Для редуцирования (сокращения) контролируемого пространства, характеризуемого пространственно-временной и топологической неоднородностью, представим ИТКС развивающейся системой, построенной на основе кластерной технологии, где каждый кластер (сегмент сети) с учетом эволюционного развития и динамичности структуры можно представить совокупностью зон мониторинга  $Z_v(t)$ , разделенных на критически важные элементы (КВЭ), масштабируемые на любом этапе развития (рис. 1).

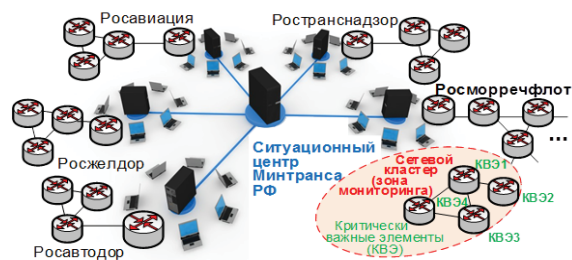


Рис. 1. Гиперграф топологической взаимосвязи зон мониторинга на примере ИТКС Министерства транспорта РФ

Из изложенного следует, что наблюдаемая ИТКС комплексируется и агрегируется в процессе эволюции в одну общую систему, что предполагает соответствующее развитие ее свойства контролируемости:  $Y(t) = \{H_v(t), L_d(t)\}$ ,  $H_v(t) = \{Z_v(t), J_p(t)\}$ , где  $H_v(t)$  – множество вершин гиперграфа (с учетом большой размерности совокупности сетевых элементов, объединенных в кластеры (зоны мониторинга) и их структуры,  $v = \overline{1, x}$ ), представляемых, к примеру, на рис. 1, федеральными агентствами (Росморречфлот, Росавиация, Росавтотдор, Росжелддор) и службой Ространснадзора, т. е.  $x \leq 5$ ;  $L_d(t)$  – множество дуг гиперграфа, представляемых  $d$ -взаимосвязями между сетевыми элементами;  $J_p(t)$  – множество дуг гиперграфа, представляемых из  $p$  отношений между КВЭ в зонах мониторинга.

На основе изложенного подхода контролируемые неоднородные сетевые элементы ИТКС представляются упорядоченной по значимости совокупностью зон мониторинга, под которыми следует понимать кластеры ИТКС с разной степенью неоднородности, состоящие из КВЭ. При этом КВЭ могут быть как однородными (например, коммутаторы), но образовывать разные, не связанные непосредственно зоны мониторинга, так и разнородными (например, для Росморречфлота – оборудование связи, контрольно-корректирующие станции дифференциальной навигационной подсистемы, базовые станции автоматической идентификационной системы и т. п.), образующими непосредственно связанные зоны. При этом КВЭ представляется технологическим ресурсом,



состоящим из неоднородных сетевых элементов, отказ которых приводит к тому, что объект контроля (ОК) полностью переходит из предотказного (предаварийного) в неработоспособное (аварийное) состояние:  $Z_1(t) = \{K_{vg}(t); g = 1, 2, \dots, m(t), \dots, l(t)\}$ , где  $K_{vg}(t)$  – совокупность из  $g$  КВЭ, причем  $m$  – необходимое и достаточное число КВЭ, а  $l$  – общее число КВЭ в процессе мониторинга ИТКС.

Предлагается следующее определение критически важного элемента как элемента агрегации сетевых устройств относительно подсистемы мониторинга ИТКС: это отдельные элементы ИТКС на различных уровнях ее разукрупнения, показатели надежности которых в наибольшей степени влияют на показатели надежности всего сетевого кластера (зоны мониторинга). Относительно контролируемого пространства КВЭ представляются сетевыми элементами с «разукрупнением вниз», контрольный опрос «ниже» которых может быть нецелесообразен. Тогда в качестве ограничений и допущений в работе предложено: обнаружение и идентификацию аварийных ситуаций в процессе мониторинга состояния ИТКС проводить в зонах мониторинга, ограничиваясь КВЭ, обеспечивающим функционирование других элементов, согласно топологии подконтрольного пространства, в пределах рассматриваемых зон мониторинга. Основываясь на результатах анализа функционирования ИТКС, каждый КВЭ имеет свою топологическую структуру. Возможна нумерация КВЭ с учетом принадлежности их к зоне мониторинга, что позволяет помимо редуцирования образовывать счетное контролируемое пространство, функционирующее на разных организационно-технических уровнях. Взаимодействие подсистемы мониторинга с конкретным КВЭ соответ-

ствующих зон мониторинга без проведения опроса всего оборудования при поиске отказа на разных уровнях разукрупнения ИТКС позволяет значительно экономить время и материальные ресурсы (рис. 2).

За счет предложенной структуры подсистемы мониторинга ИТКС, состоящей из определенных зон мониторинга, которые имеют в качестве пограничных элементов КВЭ (центры сопряжения, узлы коммутации, маршрутизаторы и пр.), можно осуществлять мониторинг сети более эффективно. Такое представление контролируемого пространства дает возможность рассматривать концептуальную модель мониторинга для определения соответствия эксплуатационных параметров средств телекоммуникаций установленным требованиям, объединяя концепции измерений, анализа и тестирования. Особенностью предлагаемого ситуационного управления является процесс передачи ИИ о состоянии КВЭ в зонах мониторинга ИТКС (зона связи, зона навигации, линии связи и пр.) для последующего анализа, что позволит обеспечивать управление системой, ее элементами и осуществлять диагностику, а при необходимости – реконфигурацию ИТКС (дистанционный переход на резерв, переключение каналов, ввод новых элементов в сеть или вывод их из эксплуатации и т. д.).

На этой основе возможно своевременное обнаружение и устранение неисправностей – от автоматического процесса сбора ИИ до выработки и принятия решений в СППР СЦ (ЕЦУ ДС, ЕЦУ ДП, ЕЦУ ВД), представляющих собой человеко-машинные системы, что повышает оперативность, точность (за счет исключения человеческого фактора) и в целом дает прирост устойчивости ее функционирования.

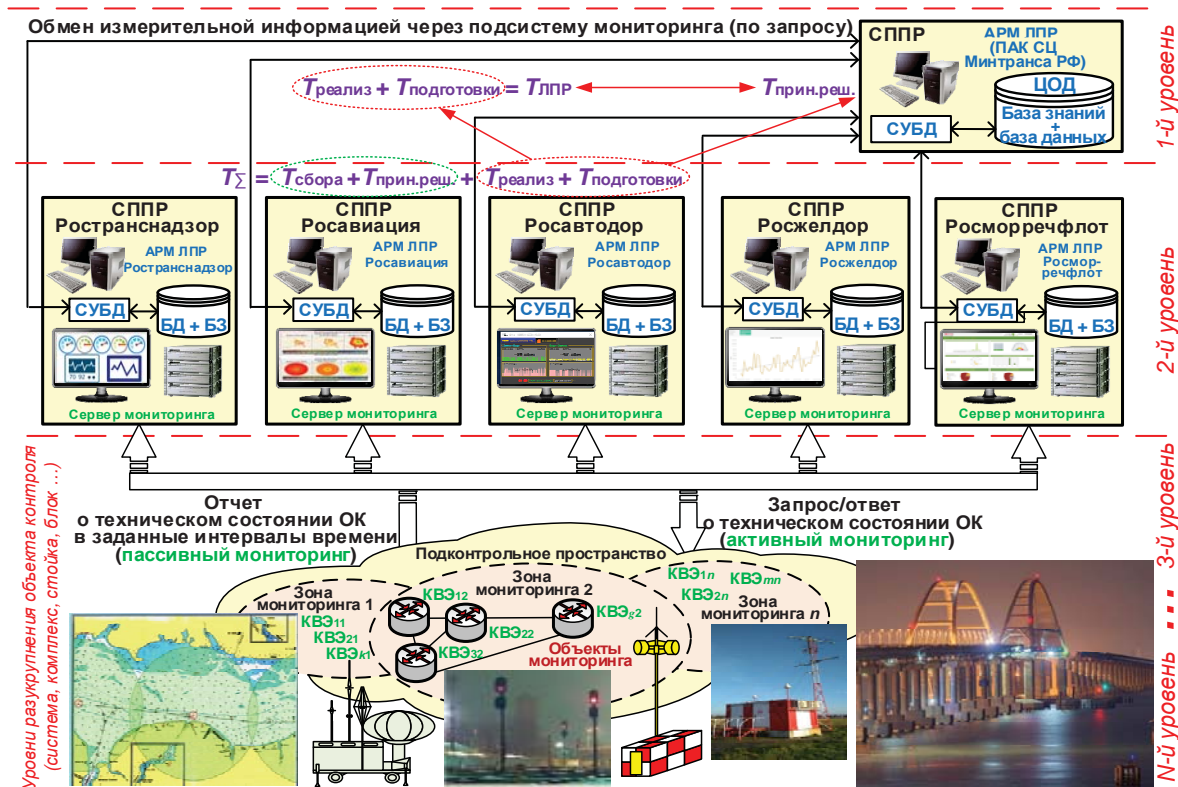


Рис. 2. Структура подсистемы мониторинга ИТКС ОП (на примере ситуационного центра Минтранса РФ)

Описание контролируемой ИТКС в терминах зон мониторинга и КВЭ, редуцирующих (снижающих размерность) подконтрольное пространство до значимого элемента, позволит осуществлять сбор ИИ о техническом состоянии (ТС) сетевых элементов помимо лиц, принимающих решения (ЛПР) СЦ уровня ведомства (или департамента), а также в автоматическом режиме проводить анализ и обработку полученной ИИ на уровне межсерверного взаимодействия, что повысит оперативность мониторинга. Для повышения достоверности ИИ о ТС КВЭ предлагается расширить количество видов ТС (включая предотказное), классифицируя их до шести [10]. При этом свойства КВЭ в зонах контроля  $W(t)$  можно характеризовать квалиметрическими параметрами  $B_{kg}(t)$ . Таким образом, расширение числа классов ТС позволит не только осуществлять прогноз состояния ОК, но и более гибко учитывать применение методов их оценки. Такая совокупность предложений позволит на концептуальном уровне редуцировать пространство мониторинга и обеспечивать доставку ИИ до СППР за минимальное время  $W(t) = \{B_{kg}(t), k = 1, 2, \dots, s(t), \dots, q(t)\}$ , где  $s(t) = 6$  – необходимое и достаточное число квалиметрических параметров, полученных путем классификации областей работоспособности КВЭ с использованием метода распределенного многоуровневого контроля [11].

На основе результатов мониторинга принимаются управляющие решения по использованию материальных и временных ресурсов для процедуры мониторинга и дальнейшего управления ИТКС. Причем в соответствии с выражением  $U_{\Sigma}(t) = R_{\Sigma}^v(t) - R_g^z(t)$  управление является функцией времени  $U_{\Sigma}(t)$  в зависимости от суммарного расходуемого ресурса с учетом времени  $t_k \ll t_k^{\text{доп}}$ , необходимого на проведение контроля сетевых элементов, где  $R_{\Sigma}^v(t)$  – суммарный ресурс ОК и подсистемы мониторинга высшего уровня управления (ведомства),  $R_g^z(t)$  – «зональный» ресурс в рамках зоны мониторинга, определяемый числом в ней КВЭ. Очевидно, что ограничение на «зональный» ресурс включает ограничение и на время, расходуемое на контроль ТС элементов сети, расположенных ниже КВЭ. Ограничивая контролируемое пространство до КВЭ приоритетных зон мониторинга, ЛПР получает временной выигрыш на принятие оперативных решений по управлению ИТКС. Данные особенности ОК составляют основу методов интеллектуального контроля, являющихся «нечувствительными» к свойству постоянного эволюционирования (совершенствования) и неоднородности ведомственных и межведомственных ИТКС. Разработка таких методов должна охватывать процессы формирования, оценки и передачи ИИ с целью принятия оперативных решений по результату аварии для обеспечения устойчивого функционирования ИТКС. Исходя из свойств автономности функционирования, топологической и пространственно-временной неоднородности, проявляющихся на гетерогенных ИТКС, процесс контроля их ТС должен осуществляться в режиме реального времени, а их подсистемы мониторинга – проектироваться с учетом адаптации к внешним факторам и внутренним режимам функционирования.

Описание подконтрольного пространства эволюционирующих (изменяющихся) ИТКС и многоуровневая структура телекоммуникационных систем предполагают их разукрупнение в зависимости от степени топологической неоднородности на зоны мониторинга с КВЭ, рис. 2. На основе организационно-технических структур примером уровней разукрупнения для Минтранса РФ (1 уровень) являются департаменты (агентства и службы) со своими ИТКС (2 уровень), ниже идут структуры, определяемые родовыми признаками

предназначения, например для Росморречфлота – структуры морского и речного флота с разбиением на администрации бассейнов ВВП РФ, взаимодействующих с ЕЦУ ДС, и далее – на районы водных путей и судоходства (как *низовой уровень*), обеспечивающие эффективное функционирование средств телекоммуникационного и навигационного оборудования на ВВП РФ.

Статический и динамический характер функционирования ИТКС на всех уровнях разукрупнения, в зависимости от смены вариантов применения (день/ночь, начало и окончание навигации и пр.) и режимов работы, определяет вариативность ее свойств, характеризуемых протекающими в ОК процессами, что выражается в виде пространственно-временной неоднородности. С учетом этого интеллектуальные методы контроля должны обеспечивать выявление зон неоднородности сетевых элементов ИТКС, проявляемых не только топологически, согласно их структуре (зон мониторинга и КВЭ), но и по протекающим в них процессам.

Синтез данных, поступающих от контролируемых сетевых элементов ИТКС, осуществляемый на основе систем их интеллектуальной обработки, поможет реализовать новое интегративное качество, позволяющее спрогнозировать и предупредить негативное развитие процессов согласно определенным законам распределения, характеризующим виды ТС (работоспособное, предотказное, неработоспособное и др.) различных КВЭ и ИТКС в целом. Но, прежде чем перейдем непосредственно к синтезу подсистемы мониторинга рассмотрим базовые понятия методов структурного синтеза и структурного анализа, используемые в последующем в формируемой методике.

## 2. Базовые понятия методов структурного синтеза и структурного анализа ИТКС ОП

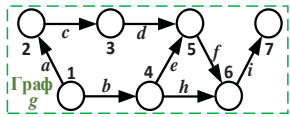
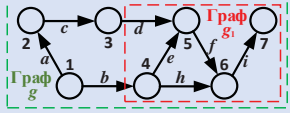
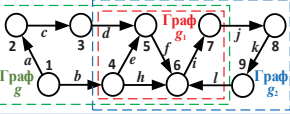
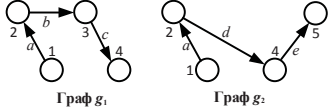
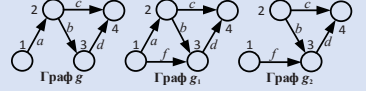
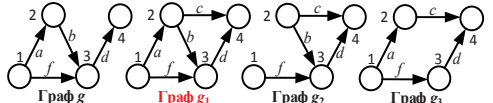
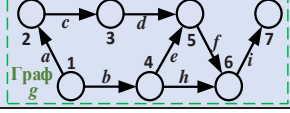
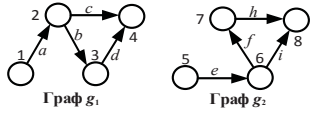
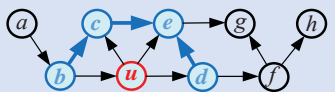
Очевидной формой представления ИТКС ОП являются графы. Узлы сети, которыми могут быть группы пользователей или отдельные клиенты и серверы, представляются вершинами графа (множество  $V$ ), а дуги графа (множество  $E$ ) представляют логические связи, например направления связи или маршруты передачи данных между узлами. Граф  $g = (V, E, \alpha, \beta)$ , описывающий сеть предполагает также наличие функции разметки узлов  $\alpha: V \rightarrow L_V$ , которую, будем считать инъективной:  $\alpha(x) = \alpha(y)$  только в случае, если  $x = y$ . В качестве меток вершин будем предполагать уникальные идентификаторы узлов. Задание графа предполагает наличие функции разметки ребер  $\beta: E \rightarrow L_E$ . В качестве меток ребер может быть использован набор следующих характеристик: ширина полосы пропускания (максимальное, минимальное, среднее); односторонняя задержка (максимальное, минимальное, среднее); объем переданных данных.

Для рассмотрения подхода к оценке динамики сети как единого целого необходимо ввести понятие графа измерений, представляющего собой граф топологии сети, взвешенный множеством измеренных значений сетевых элементов и связей (каналов, соединений). Этот подход активно используется в настоящее время при анализе сцен и распознавании изменяемых образов (лиц, отпечатков пальцев и пр.) и дает весьма обнадеживающие результаты.

Для диагностики аномального состояния сети в таблице 1 рассмотрен базовый перечень граф-метрик (расстояний между графами)  $d(g, g')$ , на основании которых сформулированы шаги выполнения операций, используемые в последующем в предлагаемой методике.

Таблица 1

Базовые понятия методов на основе расстояния редактирования графов

Определения	Графическое представление
<p><b>Определение 1.</b> Пусть дан граф <math>g=(V,E,\alpha,\beta)</math>, где <math>V</math> – множество вершин, <math>E</math> – множество ребер, <math>\alpha</math> и <math>\beta</math> соответствуют функциям разметки вершин и ребер. Тогда <math>\alpha: V \rightarrow L_V</math>; <math>\beta: E \rightarrow L_E</math>, соответствуют множествам <i>меток узлов</i> <math>L_V</math> и <i>меток ребер</i> <math>L_E</math>. Размеченный граф: <math>g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}</math>.</p>	
<p><b>Определение 2.</b> Пусть даны графы <math>g=(V,E,\alpha,\beta)</math> и <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math>. <math>g_1</math> <i>подграф</i> <math>g</math> если <math>V_1 \subseteq V, E_1 \subseteq E, \alpha(x) = \alpha_1(x), \beta(x,y) = \beta_1(x,y)</math> для любых <math>x</math> и <math>y</math>. <math>g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}</math>. <math>g_1 = \{\alpha(4, 5, 6, 7); \beta(e, f, h, i)\}</math>. Тогда: <math>g_1 \subseteq g</math>.</p>	
<p><b>Определение 3.</b> Пусть даны графы <math>g=(V,E,\alpha,\beta)</math>, <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math> и <math>g_2=(V_2,E_2,\alpha_2,\beta_2)</math>. Если <math>g_1 \subseteq g</math> и <math>g_1 \subseteq g_2</math>, то <math>g_1</math> – <i>общий подграф</i> <math>g</math> и <math>g_2</math>. <math>g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}</math>, <math>g_1 = \{\alpha(4, 5, 6, 7); \beta(e, f, h, i)\}</math>, <math>g_2 = \{\alpha(4, 5, 6, 7, 8, 9); \beta(e, f, h, i, j, k, l)\}</math>.</p>	
<p><b>Определение 4.</b> Пусть даны графы <math>g=(V,E,\alpha,\beta)</math>, <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math> и <math>g_2=(V_2,E_2,\alpha_2,\beta_2)</math>. Если <math>g_1 \subseteq g</math> и <math>g_1 \subseteq g_2</math> и не существует другого общего графа <math>g'=(V',E',\dots)</math>, такого что <math>V_1 \subset V'</math> и <math>E_1 \subset E'</math>, то <math>g_1</math> – <i>максимальный общий подграф</i> <math>g</math> и <math>g_2</math>. (<i>maximal common subgraph – MCS</i>)</p>	<p>Граф <math>g_1^{\max} = \{\alpha(4, 5, 6, 7); \beta(e, f, h, i)\}</math> является максимально общим подграфом графа <math>g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}</math> и графа <math>g_2 = \{\alpha(4, 5, 6, 7, 8, 9); \beta(e, f, h, i, j, k, l)\}</math>.</p>
<p><b>Определение 5.</b> <i>Метрика изменения (редактирования) графа</i> (graph edit distance, GED). Над графом возможно производить следующие виды операций: замена метки узла <math>\rightarrow</math> изменение состояния узла; замена метки дуги <math>\rightarrow</math> изменение состояния канала связи; вставка узла <math>\rightarrow</math> восстановление (наращивание) узлов сети; вставка дуги <math>\rightarrow</math> восстановление (добавление) канала связи; удаление узла <math>\rightarrow</math> отказ узла (деградация сети); удаление дуги <math>\rightarrow</math> отказ канала (нарушение связности – деградация сети).</p>	 <p>Расстояние между графами <math>g_1</math> и <math>g_2</math> равно 6: поскольку: удалены узел (3) и ветви (b, c); добавлены узел (5) и ветви (d, e). Следовательно расстояние редактирования <math>d(g_1, g_2) = 1 + 2 + 1 + 2 = 6</math></p>
<p><b>Определение 6.</b> Поставим в соответствие каждой операции <math>e</math> её стоимость <math>c(e)</math>. Пусть в течение времени наблюдения за сетью <math>[t, t+1]</math> граф <math>g=(V,E,\alpha,\beta)</math> перешел в граф <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math>. Тогда метрика изменения графа <math>d(g, g_1)</math> будет минимальна суммарной стоимости операций, переводящих граф <math>g</math> в граф <math>g_1</math>. <i>Минимальные графы:</i> Минимальные графы на рис.: <math>g</math> и <math>g_1, g_1</math> и <math>g_2</math> <math>d(g, g') = \min(c(s)) = \min\left\{\sum_{i=1}^N c(e_i)\right\}</math></p>	 <p><math>d(g, g_1) = 1; c(e) = 1, d(g, g_2) = 2; \sum c(e_i) = 2, d(g_1, g_2) = 1; c(e) = 1.</math> <math>d(g, g_1) = \min, d(g, g_2) = \min, \text{ а } d(g, g_1) \neq \min</math></p>
<p><b>Определение 7.</b> <i>Медианой</i> множества графов <math>G = \{g_1, g_2, \dots, g_n\}</math> называется граф <math>g'</math> такой, что суммарное расстояние от него до каждого графа минимально, т. е. граф <math>g'</math> является центром масс. Медианный граф множества <math>G = \{g, g_1, g_2, g_3\}</math> есть граф <math>g_1</math>, поскольку <math>d(g_1, g) = d(g_1, g_2) = d(g_1, g_3) = \min</math> и при этом <math>d(g_1, g_2) = d(g_1, g_3) = d(g_2, g_3) \neq \min</math>.</p>	 <p><math>\sum_{i=1}^N d(g', g_i) = \min \left\{ \sum_{i=1}^N d(g', g_i) \mid g' \in G \right\}</math></p>
<p><b>Определение 8.</b> Пусть дан граф <math>g=(V,E,\alpha,\beta)</math>. <i>Представление графа в метках</i> <math>\rho(g) = (L, C, \lambda)</math>, где: <math>L = \{\alpha(x) \mid x \in V\}</math>, <math>C = \{\alpha(x), \alpha(y) \mid (x, y) \in E\}</math>, и <math>\lambda(\alpha(x), \alpha(y)) = \beta(x, y)</math> для всех дуг <math>(x, y) \in E</math>. Размеченный граф: <math>g = \{\alpha(1, 2, 3, 4, 5, 6, 7); \beta(a, b, c, d, e, f, h, i)\}</math>.</p>	
<p><b>Определение 9.</b> Два графа <math>g=(V,E,\alpha,\beta)</math> и <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math> <i>изоморфны</i> друг другу если существуют взаимнооднозначные соответствия между множествами вершин и ребер (имеется возможность их переназначения). Изоморфные графы обладают одними и теми же свойствами и характеристиками. Графы <math>g=(V,E,\alpha,\beta)</math> и <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math> изоморфны если: существует биективная функция отображения вершин графа <math>f: V \rightarrow V_1</math>; для всех вершин имеет место равенство функций <math>\alpha(x) = \alpha_1(x)</math>; для всех ребер <math>(x, y) \in E</math>, существует такой набор <math>(f(x), f(y)) \in E_1</math>, <math>\beta(x, y) = \beta_1(f(x), f(y))</math> и для всех ребер <math>(x_1, y_1) \in E_1</math>, существует такой набор <math>(f^{-1}(x_1), f^{-1}(y_1)) \in E</math>, <math>\beta_1(x_1, y_1) = \beta(f^{-1}(x_1), f^{-1}(y_1))</math>.</p>	 <p>Граф <math>g_1</math> изоморфен графу <math>g_2</math>, поскольку <math>d(g_1, g_2) = 0</math></p>
<p><b>Определение 10.</b> <i>Соседний подграф вершины u</i> в <math>g_1=(V_1,E_1,\alpha_1,\beta_1)</math> – это подграф <math>g_1=(V'_1(u), E'_1(u), \alpha'_1, \beta'_1)</math>, где <math>E'_1(u) = E_1 \cap [N_1(u) \times N_1(u)]</math> – множество инцидентных дуг между смежными вершинами в <math>N_1(u)</math>. Граф соседей вершины <math>u</math> <math>g_1 = (V'_1(u), E'_1(u), \alpha'_1, \beta'_1), E'_1(u) = E_1 \cap [N_1(u) \times N_1(u)]</math></p>	



Исходя из данных понятий, а также изложенного в [12] будем считать, что:

граф  $g=(V,E,\alpha,\beta)$ , с представлением  $\rho(g)$ , изоморфен графу  $g_1=(V_1,E_1,\alpha_1,\beta_1)$  с представлением  $\rho(g_1)$  только и если только  $\rho(g) = \rho(g_1)$ , т. е.  $L_1 = L, C_1 = C, \lambda_1 = \lambda$ ;

граф  $g=(V,E,\alpha,\beta)$  с представлением  $\rho(g)$ , принадлежит графу  $g_1=(V_1,E_1,\alpha_1,\beta_1)$  с представлением  $\rho(g_1)$ , только и если только  $L_1 \subseteq L, C_1 \subseteq C$  и  $\lambda_1(i,j) = \lambda(i,j)$  для всех  $i,j$ , т. е.  $g_1 \subseteq g$ ;

граф  $g=(V,E,\alpha,\beta)$  с представлением  $\rho(g) = (L, C, \lambda)$  является максимальным общим графом графа  $g_1=(V_1,E_1,\alpha_1,\beta_1)$  с представлением  $\rho(g_1) = (L_1,C_1,\lambda_1)$  и графа  $g_2=(V_2,E_2,\alpha_2,\beta_2)$  с представлением  $\rho(g_2) = (L_2,C_2,\lambda_2)$ , если  $L = L_1 \cap L_2, C = \{(i,j)|(i,j) \in C_1 \cap C_2\}$ , т. е.  $MCS(g_1, g_2)$ ;

расстоянием редактирования графов  $g_1=(V_1,E_1,\alpha_1,\beta_1)$  с представлением  $\rho(g_1) = (L_1,C_1,\lambda_1)$  и  $g_2=(V_2,E_2,\alpha_2,\beta_2)$  с представлением  $\rho(g_2) = (L_2,C_2,\lambda_2)$  будет равно  $d(g_1, g_2) = |L_1| + |L_2| - 2|L_1 \cap L_2| + |C_1| + |C_2| - 2|C_0| + |C'_0|$ , при наличии максимального общего графа  $g=(V,E,\alpha,\beta)$  с представлением  $\rho(g) = (L, C, \lambda)$  когда  $L = L_1 \cap L_2, C = \{(i,j)|(i,j) \in C_1 \cap C_2\}$ , где  $C_0 = \{(i,j)|(i,j) \in C_1 \cap C_2 \text{ и } \lambda_1(i,j) = \lambda_2(i,j)\}$ , а  $C'_0 = \{(i,j)|(i,j) \in C_1 \cap C_2 \text{ и } \lambda_1(i,j) \neq \lambda_2(i,j)\}$ .

Данные выражения, следует использовать для оценки состояния сети, оценка ребер которой было уже произведено (например, по классификационной схеме «работоспособное состояние» («норма»), «неработоспособное состояние» («авария»), «предотказное состояние» («предаварийное состояние»)).

#### Взвешенные и невзвешенные расстояния на графах

Помимо приведенного в качестве меры изменения структуры сети может быть использовано следующее выражение [12]:

$$d(g, g') = 1 - \frac{|MCS(g, g')|}{MAX\{|g|, |g'|\}}, \quad (1)$$

где  $MCS(g, g')$  – максимальный общий граф  $g_1$  и  $g_2$ ,  $|g|$  – число вершин (или ребер) в графе. В качестве более сложных метрик можно использовать и другие [13, 14].

Кроме этого, для графов  $g=(V,E,\alpha,\beta)$  и  $g_1=(V_1,E_1,\alpha_1,\beta_1)$  можно использовать следующее выражение:

$$d(g, g') = |V| + |V'| - 2|V \cap V'| + |E| + |E'| - 2|E_0| + |E'|. \quad (2)$$

Как следует из теории графов, при равенстве двух графов, расстояние между ними будет минимальным и равным 0. В случае если графы не пересекаются  $g \cap g' = \emptyset$ , расстояние будет максимальным.

Однако, данные выражения следует использовать для оценки динамики структуры, сети, так как они не могут дать оценку изменения взвешенного графа, характеризуемого функциями  $\alpha, \beta$ .

Для оценки взвешенного графа также может быть использовано следующее выражение [15, 16]:

$$d(g, g') = \frac{|\beta(u, v) - \beta'(u, v)|}{\max\{\beta(u, v), \beta'(u, v)\}}. \quad (3)$$

Деление полученного выражения на общее число ребер, т. е. на  $|E \cup E'|$  позволит оценить вариацию вектора характе-

ристик ребер для графа в целом. В указанной формуле, в случае отсутствия того или иного ребра, вес последнего считается равным 0.

#### Анализ редактирования на основе спектра графов сети

Пусть задан граф  $g=(V,E,\alpha,\beta)$  с матрицей смежности вершин  $A_g$ . Спектром графа  $\sigma(g)$  назовем последовательность собственных чисел матрицы  $A_g \{\lambda_1, \lambda_2, \dots, \lambda_n\}$ .

В настоящее время известна также другая методика исследования свойств (неориентированного) графа на основе собственных чисел матрицы Кирхгофа (Лапласиан графа) [17]:  $L_g = D_g - A_g$ , где  $D_g$  – матрица степеней определяется следующим образом:

$$D_g = \text{diag} \left\{ \sum_{v \in V} \beta(u, v) \mid u \in V_g \right\}.$$

В случае невзвешенного графа, элементами матрицы  $D_g$  будут степени вершин.

В случае ориентированного графа матрица Кирхгофа определяется выражением:  $L_g = D_g - (A_g + A_g^T)$ .

На основе полученных собственных значений матрицы смежности вершин графа или матрицы Кирхгофа может быть вычислено расстояние между графами ( $GED$ ) [12]:

$$d(g, g') = \sqrt{\frac{\sum_{i=1}^k (\lambda_i - \mu_i)^2}{\min\left\{\sum_{i=1}^k \lambda_i^2, \sum_{i=1}^k \mu_i^2\right\}}}. \quad (4)$$

Для спектров графов  $\sigma(A_g) = \{\lambda_1, \lambda_2, \dots, \lambda_n\}$ ,  $\sigma(A_{g'}) = \{\mu_1, \mu_2, \dots, \mu_n\}$ ,  $k$  – эмпирически выбранный предел суммирования. В приложениях распознавания образов и обработки изображений экспериментально установлено оптимальное значение  $k = 20$ .

#### Сетевые измерения на основе структуры графа

Для вершин  $u$  и  $v$ , принадлежащих множеству вершин графа  $g (u, v \in V_g)$ , рассмотрим следующее множества путей графа:  $P_k^g(u, v)$  – путей длины  $k$ , соединяющих вершины  $u$  и  $v$ ;  $P_k^g$  – совокупность путей длины  $k$  в графе;  $P_k^g(u, v) = \bigcup_{k>2} P_k^g(u, v)$  – множество путей длины большей 2 соединяющих вершины  $u$  и  $v$ ;  $P^g = \bigcup_{k \geq 2} P_k^g$  – совокупность всех путей.

Передача данных в сети осуществляется посредством маршрутов, поэтому удаление вершины приводит к отказу маршрутов, содержащих данную вершину в качестве промежуточной. Исходя из этих соображений в качестве чувствительной метрики состояния сети можно использовать рассмотренное ранее (в табл. 1) расстояние редактирования  $GED$ , основанное на числе путей, содержащих заданную вершину(ы).

Для выделенного (непустого) подмножества ребер  $\hat{E} \subseteq E$ , сформируем новый граф  $g(\hat{E}) = (V', E', \alpha, \beta)$ , таким образом, что в исходном графе остаются только те дуги, которые содержатся в маршрутах, содержащих дуги из  $\hat{E} \subseteq E$ .



Более формально, граф  $g(\hat{E})$  формируется следующим образом:  $V' = V$ .

Ребро  $e \in E'$  тогда и только тогда, когда  $\exists p \in P_k^g : e \in p$  и  $\exists e_1 \in \hat{E}, e_1 \in p \cdot \alpha' = \alpha$ .

Веса ребер в  $G_g$  равны числу маршрутов в  $P^g$ , содержащих данное ребро в качестве компонента (и, по крайней мере, одно ребро из предопределенного набора  $\hat{E} \subseteq E$ ).

Атрибуты весов в созданном описанным способом графе  $g(\hat{E})$  отражают степень важности ребер в процессах передачи данных через сеть, и поэтому определяют степень влияния на связность узлов. Сравнение двух созданных на основе  $g_1 = (V_1, E_1, \alpha_1, \beta_1)$  и  $g_2 = (V_2, E_2, \alpha_2, \beta_2)$  графов, может быть осуществлено по формуле (2). В качестве  $\hat{E}$  выбирается  $E_1$  и  $E_2$ . Также можно использовать множество ребер максимально общего графа  $mcs(g_1, g_2)$ . Общей рекомендацией при создании  $\hat{E}$  является включение наиболее значимых связей сети.

Вариантом описанного подхода является исследование 2-компонентной связности графа. В результате смежные вершины в полученном графе соответствуют вершинам исходного графа, соединенных через общего соседа. Как результат, полученная структура более чувствительна к изменениям в топологии (включением/исключением вершин, ребер), нежели исходная структура. Однако в данном случае, граф остается невзвешенным. Сравнение полученных структур может быть произведено по формулам (1) и (2).

### Идентификация областей изменения структуры графа

При анализе динамики сети важным является не только установление факта изменения, приводящего к ошибкам, но и выявление компонент графа сети, приводящих к возникновению событий.

Расстояние между двумя графами  $g_1 = (V_1, E_1, \alpha_1, \beta_1)$  и  $g_2 = (V_2, E_2, \alpha_2, \beta_2)$  может быть охарактеризовано при помощи матрицы изменений  $C = [C_{uv}]$ , элементы которой соответствуют удаленным из  $g_1$  или добавленным в  $g_2$ . Строки и столбцы матрицы  $C$  соответствуют множеству  $V_1 \cup V_2$ . В случае удаления или добавления ребра  $(u, v)$  соответствующий элемент матрицы будет равен 1, в случае если соответствующее ребро присутствует в обоих графах, соответствующий элемент будет равен 0. Данная матрица описывает граф, называемый *симметричной разницей графов* и обозначается  $g_1 \Delta g_2$ .

Сумма элементов по строкам (или столбцам) матрицы  $C$  дает вектор изменений относительно вершин объединенного множества  $V_1 \cup V_2$ . Ранжирование с последующим выделением  $n$  максимальных компонент позволяет локализовать области изменений.

Указанный подход может быть распространен на взвешенные графы, при этом компоненты симметричной разности вычисляются по формуле:

$$C_{u,v} = \frac{|\beta(u,v) - \beta'(u,v)|}{\max\{\beta(u,v), \beta'(u,v)\}}, \quad (5)$$

где  $(u,v) \in E_1 \cup E_2$ .

Аналогично, для анализа динамики может быть использована группа симметричных разностей высшего порядка:

$$g_i \Delta^2 g_{i+2} = (g_i \Delta g_{i+1}) \Delta (g_{i+1} \Delta g_{i+2}),$$

$$g_i \Delta^3 g_{i+4} = (g_i \Delta^2 g_{i+2}) \Delta (g_{i+2} \Delta^2 g_{i+4}),$$

...

### Анализ на основе графа соседей вершин

Альтернативой симметричной разности является подход на основе измерения расстояния между соответствующими (последовательными во времени) графами соседей вершины (Определение 10 в табл. 1). Данная техника позволяет получить вектор расстояний между графами из  $g_1$  и  $g_2$ . Каждая координата вектора соответствует расстоянию между графами соседей с «точки зрения» отдельной вершины и смежных с нею вершин, что и позволяет *выявить области изменений*.

Последовательные измерения по времени состояния сети по описывающим их графам могут сравниваться с использованием вышеописанного подхода, где в качестве измерения расстояния между графами используем формулы (1-4). Граф соседей вершины, присутствующий только в одном графе, сравнивается с пустым графом. Результатом операции является вектор расстояний графов соседей вершин:

$$d = [d(g'_1(u), g'_2(u))].$$

Соседний подграф вершин описывает связи с вершинами, связанными 1 дугой. Для целей анализа целесообразно также рассмотреть 2-соседний граф, описывающий 1 и 2-компонентную связность, т. е. включающий 1 и 2 достижимые вершины, вместе с связывающими их ребрами (рис. 3).

### Средние графы

Согласно определению, медианным графом  $\bar{g}$  последовательности  $G = \{g_1, g_2, \dots, g_n\}$  называется такой граф, суммарное  $GED$  которого до каждого члена последовательности минимально:  $\bar{g} = \arg \min_{g \in U} \sum_{i=1}^n d(g, g_i)$ .

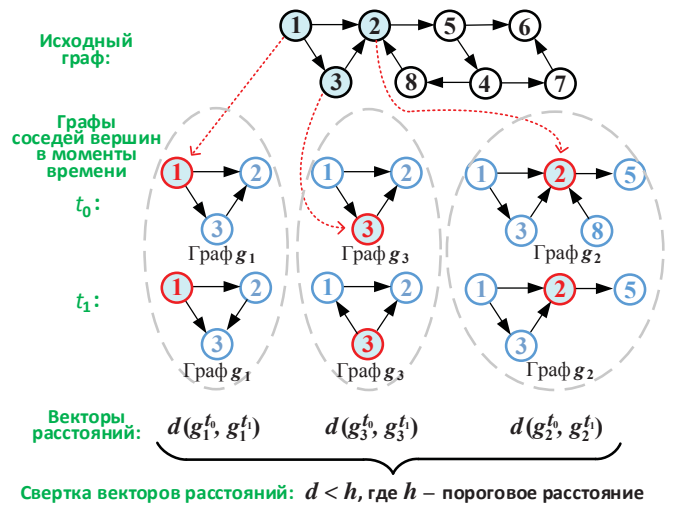


Рис. 3. Сетевые измерения на основе графов соседей

Рассмотрим  $GED$ , обобщающее формулу (1) [12]. Будем считать, что операция замены метки ребра с весом  $\beta_1(e)$  на метку с весом  $\beta_2(e)$  будет иметь стоимость  $|\beta_1(e) - \beta_2(e)|$ . В случае добавления или же удаления ребра из графа, стоимость операции будет равна весу ребра, т. е.  $|\beta_1(e) - 0|$ .

$$d_2(g_1, g_2) = c \cdot [|V_1| + |V_2| - 2|V_1 \cap V_2|] + \sum_{e \in E_1 \cap E_2} |\beta_1(e) - \beta_2(e)| + \sum_{e \in E_1 \setminus (E_1 \cap E_2)} \beta_1(e) + \sum_{e \in E_2 \setminus (E_1 \cap E_2)} \beta_2(e) \quad (6)$$

Константа  $c$  позволяет учитывать величину влияния операций вставки/удаления узлов по отношению к операции над ребрами графа.

Рассмотрим объединенный граф  $g = (V, E, \alpha, \beta)$  последовательности  $G = \{g_1, g_2, \dots, g_n\}$ , где  $V = \bigcup_{i=1}^n V_i$ ,  $E = \bigcup_{i=1}^n E_i$  и обозначим через  $\gamma(u_i)$  число повторений вершины  $u_i$  в последовательности графов.

Определим граф  $\hat{g} = (\hat{V}, \hat{E}, \alpha, \hat{\beta})$  следующим образом:

$$\begin{aligned} \hat{V} &= \{u \mid u \in V \text{ и } \gamma(u) > n/2\} \\ \hat{E} &= \{(u, v) \mid u, v \in \hat{V}\} \\ \hat{\beta}(u, v) &= \text{med}(\beta_i(u, v) \mid i = 1 \dots n) \end{aligned} \quad (7)$$

Согласно теореме, доказанной в [12], данный граф является медианным (средним) по  $GED$ , вычисляемому по формуле (6). Он не является уникальным, так как операция вставки-замены узла позволяет получить семейство средних графов.

### Применение средних графов для выявления аномальных состояний сети

Усреднение последовательности графов позволяет исключить влияние случайных флуктуаций, что подобно действию суммирующего фильтра при размытии сигнала. Поэтому данный метод, в отличие от выше рассмотренных более предпочтителен для выявления долговременных тенденций в поведении сети.

#### Сравнение среднего графа с последующим одиночным ( $msa$ )

В данном процессе производится вычисление среднего графа по «скользящему окну» длиной  $L$  (рис. 4).

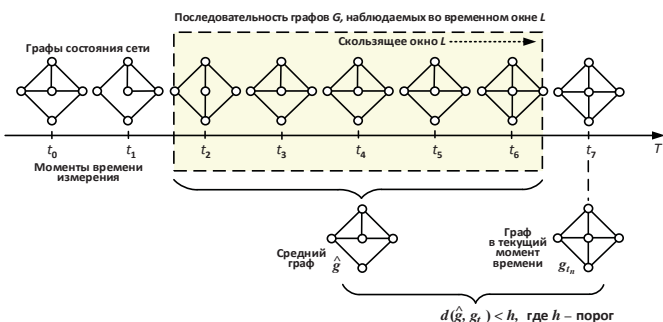


Рис. 4. Процедура  $msa$  – сравнение (измерение) среднего графа с последующим одиночным

Пусть  $\hat{g}$  – средний граф последовательности  $G = \{g_{n-L+1}, g_{n-L+2}, \dots, g_n\}$ . Тогда расстояние,  $d_2(\hat{g}, g_{n+1})$ , в сравнении с

предопределенным порогом может быть использовано для выявления аномальных (скачкообразных) изменений в поведении сети. В качестве порога можно использовать среднее изменение  $GED$  сети по скользящему окну:

$$\varphi = \frac{1}{L} \sum_{i=n-L}^n d_2(\hat{g}_n, g_i).$$

Событие «аномальное поведение сети» генерируется при условии:  $d_2(\hat{g}_n, g_{n+1}) \geq \alpha \cdot \varphi$ .

Как было указано, средний граф не является уникальным, в связи с чем, если было получено семейство средних графов  $(\hat{g}_1, \hat{g}_2, \dots, \hat{g}_m)$ , можно вычислить набор пороговых значений  $(\varphi_1, \varphi_2, \dots, \varphi_m)$ .

Решение о состоянии сети можно определить из следующего условия:

$$d_2(\hat{g}_n, g_{n+1}) \geq \alpha \cdot \varphi_1 \wedge d_2(\hat{g}_n, g_{n+1}) \geq \alpha \cdot \varphi_2 \wedge \dots \wedge d_2(\hat{g}_n, g_{n+1}) \geq \alpha \cdot \varphi_m.$$

#### Сравнение среднего графа с последующим средним ( $tta$ )

В схеме, представленной на рис. 5 в последовательных скользящих окнах  $L_1 = \{g_{n-L+1}, \dots, g_n\}$  и  $L_2 = \{g_{n-L+1}, \dots, g_{n+L+2}\}$  вычисляются средние графы  $\hat{g}_n$  и  $\hat{g}_{n+1}$ . В качестве правила принятия решения о состоянии сети

используется уравнение:  $d_2(\hat{g}_n, \hat{g}_{n+1}) \geq \alpha \cdot \left[ \frac{L_1 \varphi_1 + L_2 \varphi_2}{L_1 + L_2} \right]$ .

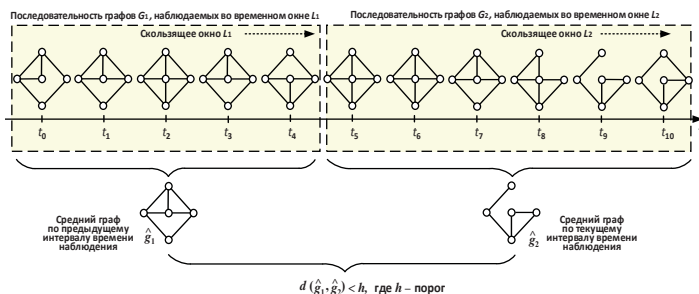


Рис. 5. Процедура  $tta$  – сравнение (измерение) среднего графа с последующим средним

#### Сравнение среднего графа с удаленным одиночным ( $msd$ )

В случае, если имеет место постепенное изменение состояния сети, целесообразно сравнивать средний граф  $\hat{g}_n$  не с последующим  $g_{n+1}$ , а с отстоящим на  $l$  измерений, где  $l$  выбирается эвристически (рис. 6).

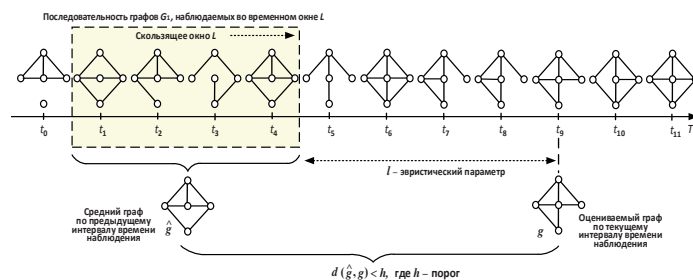


Рис. 6. Процедура  $msd$  – сравнение (измерение) среднего графа с последующим одиночным

*Сравнение среднего графа с удаленным средним (mmd)*

Данный метод представляет собой комбинацию предыдущего случая и сравнения последовательных средних. Как описано выше, рассмотрим средний граф  $\hat{g}_1$  по множеству  $G_1 = \{g_{n-L+1}, \dots, g_n\}$  и  $\hat{g}_2$  по множеству  $G_2 = \{g_{n+1}, \dots, g_{n+L}\}$ . Сравнение удаленных друг от друга граф-измерений позволяет оценить абсолютную величину «поэтапного» изменения состояния сети (рис. 7).

Рассмотренные выше процедуры (*msa*, *mma*, *msd* и *mmd*) применения средних графов для выявления аномальных состояний сети заимствованы из теории графов, активно применяемой на сегодня в интеллектуальных системах распознавания образов (распознавание лиц, жестов рук, отпечатков пальцев, радужной оболочки глаз и пр.). При этом для идентификации состояния сетевой инфраструктуры в результате сбора ИИ в каждый из моментов времени наблюдения (мониторинга)  $t$ ,  $t+1$ ,  $t+2$ , и т. д. строятся графы сети и производятся измерения расстояний между графами соседей. Таким образом, метрикам изменения (редактирования) графов в динамике (во времени) можно поставить в соответствие идентификацию следующих состояний элементов претерпевающей изменения на этапе ЖЦ динамической ИТКС: замена метки узла → изменение состояния узла; замена метки дуги → изменение состояния канала связи; вставка узла → восстановление (наращивание) узлов сети; вставка дуги → восстановление (добавление) канала связи; удаление узла → отказ узла (деградация сети); удаление дуги → отказ канала (нарушение связности – деградация сети).

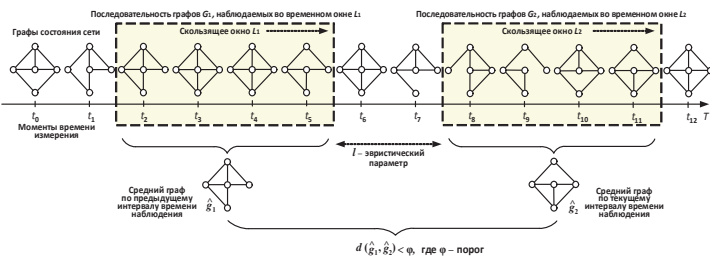


Рис. 7. Процедура *mmd* – сравнение (измерение) среднего графа с удаленным средним

Определяются метрики изменения двух соседних графов  $g$  и  $g_1$  анализируемой сети графовым расстоянием  $d(g, g_1)$ . При этом на последовательности нескольких графов  $G = \{g_1, g_2, \dots, g_n\}$ , наблюдаемых в скользящем временном окне подсистемы сетевого мониторинга, определяется минимальный граф (с минимальной суммарной стоимости операций, переводящих граф  $g$  в граф  $g_1$ ), являющийся медианным или средним графом. По изменению графа соседей вершины в различные моменты времени формируется вектор расстояний между графами соседей, которые сравниваются с пороговым значением. В случае превышения порога графового состояния на очередном временном интервале наблюдения идентифицируется изменение состояния сети (переход сети из одного вида технического состояния к другому), например деградация или восстановление сети (предотказное состояние или авария) и т. д.

Из перечисленных методов теории графов для анализа сетевых инфраструктур наиболее приемлемы методы на основе

расстояния редактирования графов, поскольку они позволяют осуществлять оценку общего состояния сети учитывая техническое состояние, как отдельных сетевых устройств (вершин графа), соединений (ребер графа), а также путей передачи данных (ПД) (маршрутов ПД). В то же время, в архитектуру сети под эти методы необходимо включение компонента интеллектуальной обработки (рис. 8).

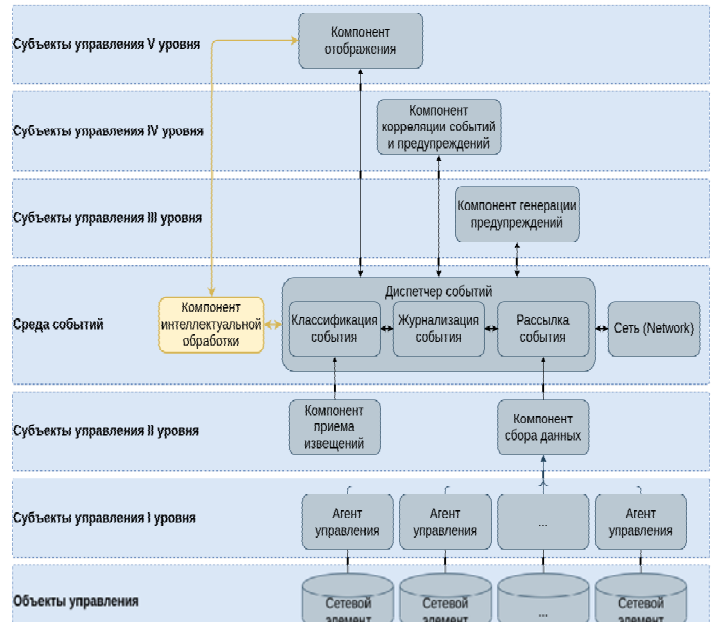


Рис. 8. Обобщенная архитектура перспективной системы мониторинга

**3. Параметрический синтез подсистемы мониторинга ИТКС ОП**

Формируемая в ходе структурного синтеза подсистема мониторинга Минтранса РФ в различных ее проявлениях должна определить исходные данные для решения задачи параметрического синтеза при сопряжении аппаратных и канальных ресурсов сегментов ИТКС. Поскольку идентификация предотказного состояния сети предусматривает принятие управленческих решений (ситуационного управления сетью), для выработки которых ЛПР необходимо знание в режиме реального времени наличествующих сетевых ресурсов (по пропускным способностям каналов связи, числу каналов в ветвях, объемах буферной памяти в центрах коммутации, односторонних задержках и пр.). С этой точки зрения для обоснованного принятия управленческих решений на переконфигурацию сети в случае возникновения её предотказного состояния процедура этапа параметрического синтеза важна для подсистемы мониторинга.

Понятие эффективности использования ресурсов является ключевым при анализе и синтезе ИТКС и ее подсистем. Так, в некоторых источниках [2] задача синтеза сети сводится к задаче управления ее ресурсами. При этом эффективность использования ресурсов подсистемой мониторинга как сетевой структуры оценивается протекающей по ветвям ИИ по отношению к пропускным способностям (ПС) этих ветвей технологической связи.



В структурах, синтезированных по методам замены [18] ветвей, ПС каждой ветви подсистемы мониторинга берется равной проходящей по ней нагрузке. Поскольку в реальных ИТКС создающие нагрузку потоки измерительной (ИИ) и управляющей информации (УИ) являются случайными, то согласно основным результатам теории массового обслуживания (ТМО) среднее время обслуживания и длины очередей на входе в каждый канал будут стремиться к бесконечности, а вероятность потерь будет превышать все разумные пределы. Поэтому определенное превышение ПС данной ветви над протекающей по ней ИИ принципиально необходимо для обеспечения требований к качеству функционирования подсистемы мониторинга, что и является объектом оптимизации. Это означает, что эффективность использования ресурсов подсистемой мониторинга и качество мониторинга (как услуги) являются взаимосвязанными понятиями.

Как известно из ТМО, чем выше требуемое качество услуги, тем больший объем ПС необходим для ее предоставления и тем ниже эффективность использования ресурсов сети, т. е. в конкретной ИТКС с определенным набором механизмов управления производство качества услуги на эффективность есть фиксированная величина:  $Q \cdot E = C$ , где  $Q$  – абстрактное значение качества услуги, предоставляемой подсистемой мониторинга;  $E$  – абстрактное представление значения эффективности использования ресурсов подсистемы мониторинга;  $C$  – некоторая постоянная величина, характеризующая сеть с точки зрения качества мониторинга. Возникает вопрос, какие качественные показатели подсистемы можно интерпретировать как абстрактные значения качества услуг мониторинга, что относится и к понятию абстрактного значения эффективности использования ресурсов ИТКС.

Как следует из ТМО, зависимость  $Q \cdot E = C$  существует реально, если в качестве абстрактного значения эффективности использования ресурсов рассматривать величину  $\chi_i$ , определяющую комплексный коэффициент загрузки измерительно информацией технологических каналов и равную  $\chi_i = F_i / (n_i V_i)$  [19], где  $F_i$  – поток в ветви подсистемы мониторинга, связывающей узлы ее сенсорного и диспетчерского уровней  $i$  и  $j$ ;  $V_i$  – пропускная способность этой ветви;  $n_i$  – количество каналов в заданном направлении. Если положить  $U_i = n_i V_i$  канальной емкостью заданного направления, то  $\chi_i U_i = F_i$ , где  $U_i$  может выступать в качестве абстрактного значения качества услуги мониторинга с некоторыми оговорками. Произведение  $U = nV$  представляет собой ПС пучка каналов телеизмерений-телесигнализации (ТИ-ТС) в выбранном направлении передачи ИИ, необходимую для обеспечения определенного уровня мониторинга.

В общем случае очереди ИИ связаны с входом в каждый канал ТИ-ТС, образованный пучком из  $n$  каналов и коллективно используемой памятью. Применяемые для оптимизации сетей функционалы, заимствованные из ТМО, помимо ограниченности условий использования являются монотонно стремящимися к бесконечности выпуклыми функциями и не содержат экстремумов. В этой связи задача рационального использования ресурсов подсистемой мониторинга ИТКС формулируется как задача условной оптимизации, требующая задания функций стоимости, которые связывают оптимизируемые параметры функциональной зависимостью.

Справедливое желание в этих условиях как-то оптимизировать показатели качества сети привело к использованию множества разнообразных форм функций стоимости без достаточной аргументации для конкретных условий решаемой задачи. Возникло даже авторитетное мнение [20], что в качестве функции стоимости следует использовать ту, которую легче оптимизировать. Иначе говоря, отсутствие естественных уравнений связи вносит определенный субъективизм в результаты решения сетевых оптимизационных задач.

Так, проведенные исследования [20] позволили сформулировать две задачи, допускающие решения, удобные для интерпретации результатов, и в качестве уравнений связи используют естественные условия:

*первая задача* минимизации среднего времени задержки заявки (памяти) в сети при обеспечении вероятности отказа в обслуживании не более допустимой –

$$\bar{T}_{zad}^{\min} = \min_{V,F} \bar{T}_{zad}, \text{ при } \bar{P}_{otk} \leq \bar{P}_{otk}^{dop}; \quad (8)$$

*вторая задача* определения максимально допустимой вероятности отказа в обслуживании при обеспечении допустимого среднего времени задержки пакета измерительной информации –

$$\bar{P}_{otk}^{\max} = \max_{V,F} \bar{P}_{otk}, \text{ при } \bar{T}_{zad} \leq T_{zag}^{dop}. \quad (9)$$

При этом обе задачи могут рассматриваться как двойственная задача нелинейного программирования. Поэтому в данной работе каждый  $i$ -й сегмент подсистемы мониторинга ИТКС моделируется в виде системы массового обслуживания (СМО) типа  $M/M/n/m$  с ограниченной очередью ( $n$ -канальная СМО с ожиданием), на которую поступает пуассоновский поток заявок с интенсивностью  $\lambda_i$ , интенсивностью обслуживания  $\mu_i$  и числом мест в очереди для  $i$ -го сегмента сети  $m_i$ . В общем случае очереди связаны с входом в каждый сегмент, образованный пучком из  $n$  каналов и коллективно используемой памятью (объемом  $m$  ячеек) в каждом направлении системы телеизмерений-телесигнализации (ТИ-ТС).

Первая задача решена в [20] для ИТКС путем оптимизации среднего времени задержки  $\bar{T}_{zad}$  ИИ по комплексному показателю  $\chi_i$  для каждого  $i$ -го сегмента сети  $\chi_i = f(n_i, m_i)$ . В [19] предлагается решение второй задачи по оптимизации параметров подсистемы мониторинга ИТКС.

При этом необходимо отметить, что расчет величины средней максимальной вероятности отказа  $\bar{P}_{otk}^{\max}$ , предлагаемый в настоящей работе, лишен элементов субъективизма, так как определяется количественными, а не стоимостными характеристиками параметров сети  $F_j, V_i, n, m$  (величиной трафика ИИ, ПС каналов ТИ-ТС, их числом и емкостью буферной памяти), для которого ТМО дает строгие аналитические зависимости. При этом среднее число каналов, занятых измерительной информацией в каждом сегменте сети определяется [20] как

$$\bar{z}_i = \rho_i \left( 1 - \frac{\rho_i^{n_i+m_i}}{n_i^{m_i} n_i!} P_0 \right), \quad (10)$$

где  $\rho_i = \lambda_i / \mu_i$  – приведенная интенсивность потока заявок с ИИ;



$$\frac{\rho_i^{n_i+m_i}}{n_i^{m_i} n_i!} P_0 = P_{i,ok} - \quad (11)$$

вероятность отказа (потери пакета ИИ) в обслуживании очередному поступившему в узел диспетчерского уровня пакету ИИ по причине отсутствия мест в очереди;  $P_0$  – вероятность того, что каналы ТИ-ТС свободны, нет очереди и нет заявок на обслуживание в СМО:

$$P_0 = \left( \sum_{\alpha=0}^{n_i-1} \frac{(n_i \chi_i)^\alpha}{\alpha!} + \frac{(n_i \chi_i)^n}{n_i!} \frac{1 - \chi_i^{m_i+1}}{1 - \chi_i} \right)^{-1}. \quad (12)$$

Среднее число заявок, находящихся в очереди сегмента подсистемы мониторинга, найдем как

$$\bar{r}_i = P_{i,ok} \sum_{\alpha=1}^{m_i} \alpha \chi_i^{-(m_i-\alpha)}, \quad (13)$$

где  $\chi_i = \rho_i / n_i$  – степень загрузки канала  $i$ -го сегмента подсистемы мониторинга.

Тогда среднее число заявок в СМО определим как

$$\bar{W}_i = \bar{z}_i + \bar{r}_i. \quad (14)$$

С учетом (11)–(13) выражение (14) примет вид

$$\bar{W}_i = n_i \chi_i (1 - P_{i,ok}) + P_{i,ok} \sum_{\alpha=1}^{m_i} \alpha \chi_i^{-(m_i-\alpha)}. \quad (15)$$

Соотношение (15) справедливо для любого сегмента изотропной сети, в которой  $\rho$  не зависит от направления передачи ИИ в каналах ТИ-ТС и вероятности потерь в каждом  $i$ -м сегменте подсистемы мониторинга, поскольку  $\chi_i = \rho / n_i \approx \chi$ ,  $P_{i,ok} \approx P_{otk}$ .

Используя формулу Литтла и клейнроковскую аппроксимацию независимостью для  $k$  сегментов системы мониторинга ( $k=5$ : Росморречфлот, Росавиация, Росжелдор, Росавтодор, Ространснадзор, см. рис. 2) имеем:

$$\gamma \bar{T}_{zad} = k \bar{W}_i \quad (16)$$

В данном случае формула Литтла является практически единственным средством выхода на сетевой уровень OSI. Тогда с учетом выражения (16) среднее время задержки заявки (пакета ИИ) составляет

$$\bar{T}_{zad} = \frac{1}{\gamma} k [P_{otk} \sum_{\alpha=1}^{m_i} \alpha \chi^{-(m_i-\alpha)} + n \chi (1 - P_{otk})]. \quad (17)$$

Задавшись допустимым временем задержки пакета ИИ в подсистеме мониторинга, т. е.  $\bar{T}_{zad} \leq T_{zad}^{dop}$ , можно из (17) определить среднюю максимальную вероятность потери заявок (пакетов ИИ) в подсистеме мониторинга в пределах допустимого времени их задержки [2]:

$$\bar{P}_{otk}^{max} = \frac{\gamma \bar{T}_{zad} - k n_i \chi}{k \sum_{\alpha=1}^{m_i} \alpha \chi^{-(m_i-\alpha)} - k n_i \chi} \quad (18)$$

Функция (18) имеет экстремум (максимум), поиск которого является задачей безусловной оптимизации. Путем вычисления частной производной  $\partial \bar{P}_{otk} / \partial \chi = 0$  получаем абсо-

лютный экстремум, который в силу унимодальности  $\bar{P}_{otk}^{max}$  является глобальным. Данный подход абсолютно исключает субъективизм при выборе функции стоимости для конкретных условий задачи. В силу аддитивности функции (16) и условия (14) после вычисления частной производной получаем уравнение, которое является функцией одной независимой переменной (свойство сепарабельности), т. е.  $\partial \bar{P}_{otk} / \partial \chi = d \bar{P}_{otk} / d \chi = 0$ .

Для упрощения расчетов обозначим  $A = \gamma / k \cdot T_{zad}^{dop}$ , тогда (18) примет вид

$$\bar{P}_{otk} = \frac{A - n_i \chi}{\sum_{\alpha=1}^{m_i} \alpha \chi^{-(m_i-\alpha)} - n_i \chi}. \quad (19)$$

$$\text{С другой стороны, } A - n_i \chi = \frac{\sum_{\alpha=1}^{m_i} \alpha \chi^{-(m_i-\alpha)} - n_i \chi}{1 + \frac{1}{n_i} \sum_{\alpha=1}^{m_i} \alpha (m_i - \alpha) \chi^{-[m_i-(\alpha-1)]}}$$

Тогда, подставив данное выражение в (19), определим среднюю максимальную вероятность отказа для условий передачи ИИ за время  $T_{zad}^{dop}$ :

$$\bar{P}_{otk}^{max} = \frac{1}{1 + \frac{1}{n_i} \sum_{\alpha=1}^{m_i} \alpha (m_i - \alpha) \chi^{-[m_i-(\alpha-1)]}}. \quad (20)$$

С другой стороны, имеют место выражения для первой (8) и второй (9) задач оптимизации (показанных выше), которые в совокупности, с учетом (14), можно представить как

$$\bar{P}_{otk}^{max} = \frac{(n_i \chi)^{n_i+m_i}}{n_i! n_i^{m_i}} \frac{1}{\sum_{\alpha=0}^{n_i} \frac{(n_i \chi)^\alpha}{\alpha!} + \frac{(n_i \chi)^{n_i}}{n_i!} \sum_{\alpha=1}^{m_i} \chi^\alpha}. \quad (21)$$

После преобразования (21) получим:

$$\bar{P}_{otk}^{max} = \frac{1}{\frac{n_i!}{\chi^{m_i}} \sum_{\alpha=0}^{n_i} \frac{(n_i \chi)^{-(n_i-\alpha)}}{\alpha!} + \sum_{\alpha=1}^{m_i} \chi^{-(m_i-\alpha)}}. \quad (22)$$

Левые части выражений (20) и (22) равны, следовательно, правомерна следующая запись:

$$\frac{n_i!}{\chi^{m_i}} \sum_{\alpha=0}^{n_i} \frac{(n_i \chi)^{-(n_i-\alpha)}}{\alpha!} + \sum_{\alpha=1}^{m_i} \chi^{-(m_i-\alpha)} = 1 + \frac{1}{n_i} \sum_{\alpha=1}^{m_i} \alpha (m_i - \alpha) \chi^{-[m_i-(\alpha-1)]}. \quad (23)$$

После несложных преобразований (24) получаем равенство

$$\sum_{\alpha=0}^{n_i} \frac{n_i!}{\alpha!} (n_i \chi)^{-(n_i-\alpha)} = \sum_{\alpha=1}^{m_i-1} \left( \frac{\alpha (m_i - \alpha)}{n_i \chi_i} - 1 \right) \chi_i^\alpha, \quad i = \bar{1}, k. \quad (24)$$

Выражение (24) идентично полученному в [19] при оптимизации среднего времени задержки пакетов в сети в пределах допустимой вероятности их потерь, соответствующему выражению  $\bar{T}_{zad}^{min} = \min_{V,F} \bar{T}_{zad}$  при  $\bar{P}_{otk} \leq \bar{P}_{otk}^{dop}$ , т. е. первой задачи оптимизации (9). Определим корни уравнения (24), изменяющиеся в пределах  $0 \leq \chi \leq 1$  как приемлемые (*pr*) значения степени загрузки каналов  $\chi_{pr}$ , так как в соответствии с ТМО при

$\chi \geq 1$  среднее времени задержки пакетов в сети и вероятность их потерь значительно возрастают, превышая все допустимые значения.

Таким образом, полученный результат (24) позволяет говорить об однозначном соответствии приемлемых оптимальных значений степени загрузки  $\chi_{pr}^{opt}$  каналов ТИ-ТС как минимальному среднему времени задержки пакетов ИИ в подсистеме мониторинга при заданной допустимой вероятности их потерь, так и средней максимальной вероятности потерь пакетов ИИ в подсистеме мониторинга при заданном допустимом времени их задержки, зависящих, в свою очередь, как от требуемого значения вероятности потерь пакетов ИИ  $P_{отк}^{dop}$ , так и от допустимого времени их задержки  $T_{зад}^{dop}$  и являющихся функциями дискретных значений числа измерительных каналов  $n$  и числа мест в очереди  $m$ .

Уравнение системы (24) является функцией одной переменной  $\chi$  и дает возможность независимо определить приемлемое значение степени загрузки ИИ канала ТИ-ТС для каждого сегмента подсистемы мониторинга  $\chi_i^{pr}$ . Однако получить точное аналитическое решение выражения (24) не представляется возможным ввиду его трансцендентности, но оно может быть решено программно-численным методом либо графическим методом. Программно-численный метод решения не сложно реализовать с помощью программы Mathcad, которая через номограммы, представленные на рис. 9, позволяет определить приемлемые значения  $\chi_i^{pr}$  в зависимости от оптимальных значений, соответственно  $\overline{T}_{зад}^{min}$  и  $\overline{P}_{отк}^{max}$ , а также сочетаний числа каналов ТИ-ТС  $n$  и количества мест в буфере  $m$ . Причем определив значения  $\chi_{i pr}^{opt}$  и величину суммарного потока ИИ на входе  $i$ -го сегмента подсистемы мониторинга, можно определить необходимое количество каналов ИИ  $i$ -го сегмента сети и их ПС, исходя из соотношения

$$\chi_{i pr}^{opt} = \frac{\lambda_i}{n_i \mu_i} = \frac{L \lambda_i}{n_i L \mu_i} = \frac{F_i}{V n_i}; \quad \chi_{i pr}^{opt} = f(m_i, n_i). \quad (25)$$

Параметрический синтез подсистемы мониторинга по комплексному показателю  $\chi_{pr}^{opt}$  (25) позволяет варьировать величинами  $V_i$  и в зависимости от потока ИИ (класса трафика  $F_i$ ), предоставляя автоматизированным измерительным комплексам сегментов сети (Росморречфлот, Росавиация, Росжелдор, Росавтодор, Ространснадзор) любую совокупность измерительных каналов (каналов ТИ-ТС) с шириной переменных битовых скоростей передачи (ШПБСП), формируя каждый раз виртуальный канал с переменной ПС независимо от требуемого  $T_{зад}^{dop}$ , при этом вероятность отказа в обслуживании заявки (пакета ИИ) будет оставаться в пределах допустимой. Совмещение условий (11), (12), (17), (18), (24), (25), представленных на рис. 9, позволяет сделать вывод, что в пределах установленных значений параметров временной прозрачности сети можно осуществить обмен ПС канала ТИ-ТС на объем буферной памяти на входе в данный канал. Откуда следует, что такой обмен может быть осуществлен при условии поддержания постоянства таких качественных показателей подсистемы мониторинга и ее автоматизированного измерительного комплекса по сегментам се-

ти, как время задержки и вероятность потери заявок (пакетов ИИ) в допустимых пределах. Причем в случае значительной разности проектной величины для передачи телеизмерительной нагрузки между сенсорным и диспетчерским уровнями системы с целью экономии ее ресурса целесообразно при планировании используемого ресурса исходить из временной прозрачности каждого сегмента ИТКС, а не сети в целом.

Расчеты по выражениям (17), (18), (24) позволяют определить, исходя из имеющихся ресурсов в сегментах подсистемы мониторинга ( $n_i, m_i, V_{ij}$ ), ширину переменных битовых скоростей передачи, в пределах которой допустимо изменять скорость передачи в каналах ТИ-ТС, сочетая ее с необходимым количеством мест в буферной памяти сервера мониторинга сегмента ИТКС и сохраняя при этом временную прозрачность сегментов сети и ИТКС в целом. Так, на рисунке 9 для удобства показаны лишь три ШПБСП для заданного числа каналов ТИ-ТС  $n_i$  в сегментах ИТКС и требуемых для нее  $P_{отк}^{dop}, T_{зад}^{dop}$ . При этом «левые» границы ШПБСП, определяемые значениями  $m_b, V_{ij}$  на сегментах подсистемы мониторинга на рисунке 9 не приведены.

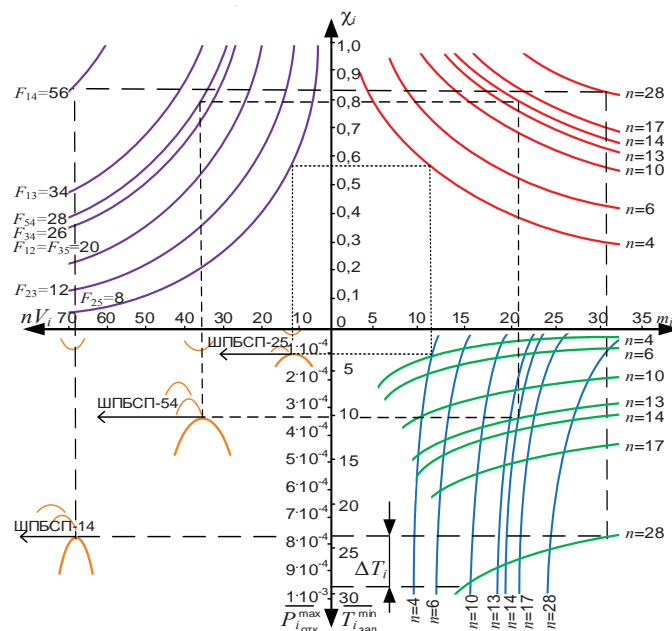


Рис. 9. Номограммы согласования параметров и характеристик подсистемы мониторинга СЦ Минтранса РФ

#### 4. Разработка методики синтеза подсистемы интеллектуального мониторинга ИТКС ОП

Процедура мониторинга современных сетевых инфраструктур должна осуществляться в режиме реального времени. При этом если в момент времени  $t$  состояние наблюдаемой сети принять за исходное состояние (первое множество вершин и ребер на сетевом графе  $g$ ), то в промежуток времени  $t + 1$  в силу внутренних (изменение режимов работы, величины обрабатываемого трафика и пр.), а также внешних (ошибки обслуживающего персонала, дестабилизирующие воздействия и пр.) на динамической структуре будет наблюдаться совершенно другое состояние (второе

множество вершин и ребер сетевого графа  $g_1$ ), в момент времени  $t + 2$  может наблюдаться третье состояние, описываемое сетевым графом  $g_2$ , или сеть может вернуться в исходное состояние, описываемое сетевым графом  $g$  и т. д. Каждое из этих состояний характеризуется расстоянием между графами  $d(g, g_1)$ ,  $d(g, g_2)$  и т. д. Если исходное состояние сети, описываемое графом  $g$  принять за эталонное и определить порог на изменение расстояния между ним и новыми графами, образующимися в моменты времени  $t + 1$ ,  $t + 2$  и т. д., как и порог на суммарное расстояние от него до каждого образованного графа, то в случае превышения величины порога будем считать, что сеть перешла в другое состояние. Нормальное состояние ИТКС характеризуется допустимыми изменениями топологии сети, что описывается некоторым множеством графов, также как и другие виды состояний ИТКС определяются также некоторым множеством графов. Данные множества образуют кластеры, в которых средний граф будет являться центром кластера (центром масс).

Эффективность работы алгоритмов кластеризации обычно оценивают с помощью двух параметров: временной и/или пространственной сложности. Так в работе [21] предлагается оценка алгоритмов кластеризации, предназначенных для обработки числовых данных ( $k$  – средних,  $EM$ , метод ближайшего соседа,  $EM$ -модифицированный и  $FarthestFirst$ ). С этой целью было сгенерировано множество искусственных тестовых наборов данных. Объекты данных представлены точками в двухмерном евклидовом пространстве. Тестовый набор данных – это множество групп данных, называемое исходными кластерами. В ходе тестирования алгоритмов кластеризации были произведены измерения времени выполнения алгоритмов и объема оперативной памяти, использованной алгоритмом в ходе выполнения задачи (табл. 2). При этом в [21] приводится алгоритм оценки качества кластеризации, по которой анализируемые алгоритмы кластеризации имеют следующие индексы качества:  $EM$ -алгоритм – 0,9;  $EM$  (модифицированный) – 0,6;  $Farthest First$  – 0,48;  $k$ -средних – 0,85; метод ближайшего соседа – 0,32.

Из результатов тестирования оценено качество кластеризации на основе процедуры установок контрольных значений в объектах кластеризации и последующего вычисления индекса качества кластеризации. Лучшие показатели индекса качества выявлены у алгоритмов  $EM$  и  $k$ -средних: 0,9 и 0,85 соответственно. Однако алгоритм  $k$ -средних выполняется в среднем в 10 раз быстрее алгоритма  $EM$ . Поэтому при обработке больших объемов числовых данных предпочтительней использовать алгоритм  $k$ -средних. При этом, если в ходе обработки наблюдаемых временных рядов параметров метрик, получаемых от сетевых устройств, используется  $EM$ -алгоритм [22], то для обучения классификатора определения состояния

всей сети в-целом наиболее подходит алгоритм  $k$ -средних (как невероятностный аналог  $EM$ -алгоритма).

С учетом вышеизложенного, а также на основании понятия среднего графа (Определение 7 табл. 1) для идентификации видов состояния ИТКС можно применить алгоритм  $k$ -средних.

В то же время, в разрабатываемой методике не совсем корректно говорить о применении  $EM$ -алгоритма, либо алгоритма  $k$ -средних, по всей видимости надо вести речь о построении классификатора на основе методологии, используемой в процедуре алгоритма  $k$ -средних с несколькими существенными оговорками:

во-первых, обучение классификатора состояния сети на практике используется не так часто (на этапах вода сети в эксплуатацию, модернизации (наращивания) сети, отработки новых режимов функционирования оборудования и пр.), поэтому большой объем вычислений при обучении классификатора не столь критичен, в тоже время, если сеть часто меняет структуру, то алгоритм  $k$ -средних предпочтительнее по быстродействию;

во-вторых, в классическом алгоритме  $k$ -средних работа ведется над точками Евклидова пространства, а в предлагаемой методике речь идет о графовом пространстве с метриками в виде графовых расстояний;

в-третьих, в  $EM$ -алгоритме (в его метрическом пространстве) можно сказать, что в каждом кластере точки распределены по некоторому закону распределения случайной величины (метрики), а для графового пространства, это пока еще не однозначно, необходим поиск закономерностей изменения графов сети;

в-четвертых, в качестве исходных данных для идентификации класса в  $EM$ -алгоритме и алгоритме  $k$ -средних используются облака данных как неупорядоченные наборы данных, не привязанные к какой-либо из шкал измерений, а в предлагаемой алгоритме облако данных представляют в виде множества точек в заданном топологическом пространстве метрик графов, описывающих состояния ИТКС во времени.

Однако, поскольку предлагаемый алгоритм методики в основе своей использует методологию кластеризации, используемую в процедуре алгоритма  $k$ -средних, то это можно считать его модификацией.

Блок-схема алгоритма методики синтеза подсистемы интеллектуального мониторинга ИТКС приведена на рисунке 10. При этом алгоритм состоит из этапа структурного синтеза, этапа параметрического синтеза и этапа структурного анализа, обеспечивающего процедуру обучения классификатора по модифицированному алгоритму  $k$ -средних и непосредственно процесс идентификации состояния сети. Рассмотрим эти этапы по шагам.

Таблица 2

Тестирование алгоритмов кластеризации по измерению памяти и измерению времени [21]

Алгоритм кластеризации	Пространственная сложность (измерение памяти), Мбайт								Временная сложность, секунды							
	750	000	1500	2000	2500	3000	10000	50000	750	1000	1500	2000	3000	10000	0000	
<i>FarthestFirst</i>	0,23	0,36	0,29	0,37	0,50	0,58	1,67	3,62	0,01	0,06	0,01	0,01	0,04	0,07	0,2	
$k$ -средних	0,90	,08	,93	3,56	1,91	0,74	2,69	16,59	0,01	0,07	0,11	0,26	0,41	1,95	,23	
$EM$	1,09	1,45	3,13	4,68	1,60	5,24	9,03	35,37	0,47	1,2	2,31	2,74	4,66	20,22	124,07	
$EM$ (модифицированный)	1,57	,98	,16	5,52	3,36	5,69	11,64	45,05	1,45	2,24	5,5	11,4	23,31	298,95	9049	
Метод ближайшего соседа	24,57	54,08	97,09	206,93	294,91	386,22	1103,33	2837,38	18	75	124	219	477	900	34122	



**Этап структурного синтеза:**

на шаге 1 в соответствии с ГОСТ 27.002-2015 (Рек. ИТУ-Т М.3703) устанавливают виды состояния ИТКС и возможных ее режимов работы, минимальную ширину скользящего окна анализа  $L_{\min}$ , задают пороги  $\varphi$  на уровень деградации сетевой инфраструктуры в виде расстояния между графами  $d(g, g_1)$ , а также требуемые значения параметров (метрик) и вероятностно-временных характеристик (ВВХ) обмена ИИ в системе мониторинга;

на шаге 2 реализуют серверами мониторинга функцию выборки – получают актуальное описание сети;

на шаге 3 представляют подсети и сегменты сети совокупностью зон мониторинга, разделенных на КВЭ, подвергаемые мониторингу (ниже которых осуществлять мониторинг нецелесообразно);

на шаге 4 реализуют функцию назначения – закрепление каждого сетевого элемента (КВЭ) в соответствии с матрицей тяготения не менее чем двумя серверами мониторинга (принцип децентрализации);

на шаге 5 представляют сеть телеизмерений (систему мониторинга), неориентированным графом.

**Этап параметрического синтеза:**

на шаге 6 реализуют функцию проверки связи – проверки назначенного списка сетевых устройств для оценки их быстродействия, времени безотказной работы и расстояния до сети

(передача/прием пакетов – ring). Данная опция позволяет осуществить разметку вершин и ребер сетевого графа, получить взвешенный граф сети;

на шаге 7 реализуют функцию сбора значений параметров (метрик) через выполнение запросов к сетевым устройствам, которым назначен сервер мониторинга, и запись ИИ в распределенную базу данных (БД) знаний (БЗ);

на шаге 8 рассчитывают основные параметры и ВВХ подсистемы мониторинга для недогруженного, нагруженного и перегруженного режима функционирования ИТКС. При этом пользуются процедурой (8) – (22);

на шаге 9 осуществляют построение номограммы согласования параметров и ВВХ обмена ИИ в системе мониторинга, когда по комплексному показателю  $\chi$  рассчитывают необходимые для неё параметры сети ИИ-ТС;

на шаге 10 определяют приемлемые наборы параметров и ВВХ обмена ИИ для заданного назначения серверам мониторинга элементов сети при текущем режиме ее загрузки:  $\chi = 0...0,4$  – недогруженный;  $\chi = 0,4...0,8$  – нагруженный;  $\chi = 0,8...1,0$  – перегруженных, с записью данных параметров в распределенную БД (БЗ) для последующего их использования как в интересах подэтапа идентификации состояния сети, так и выработки управляющих воздействий СППР на переконфигурацию сети при наличии параметрических изменений на ней.

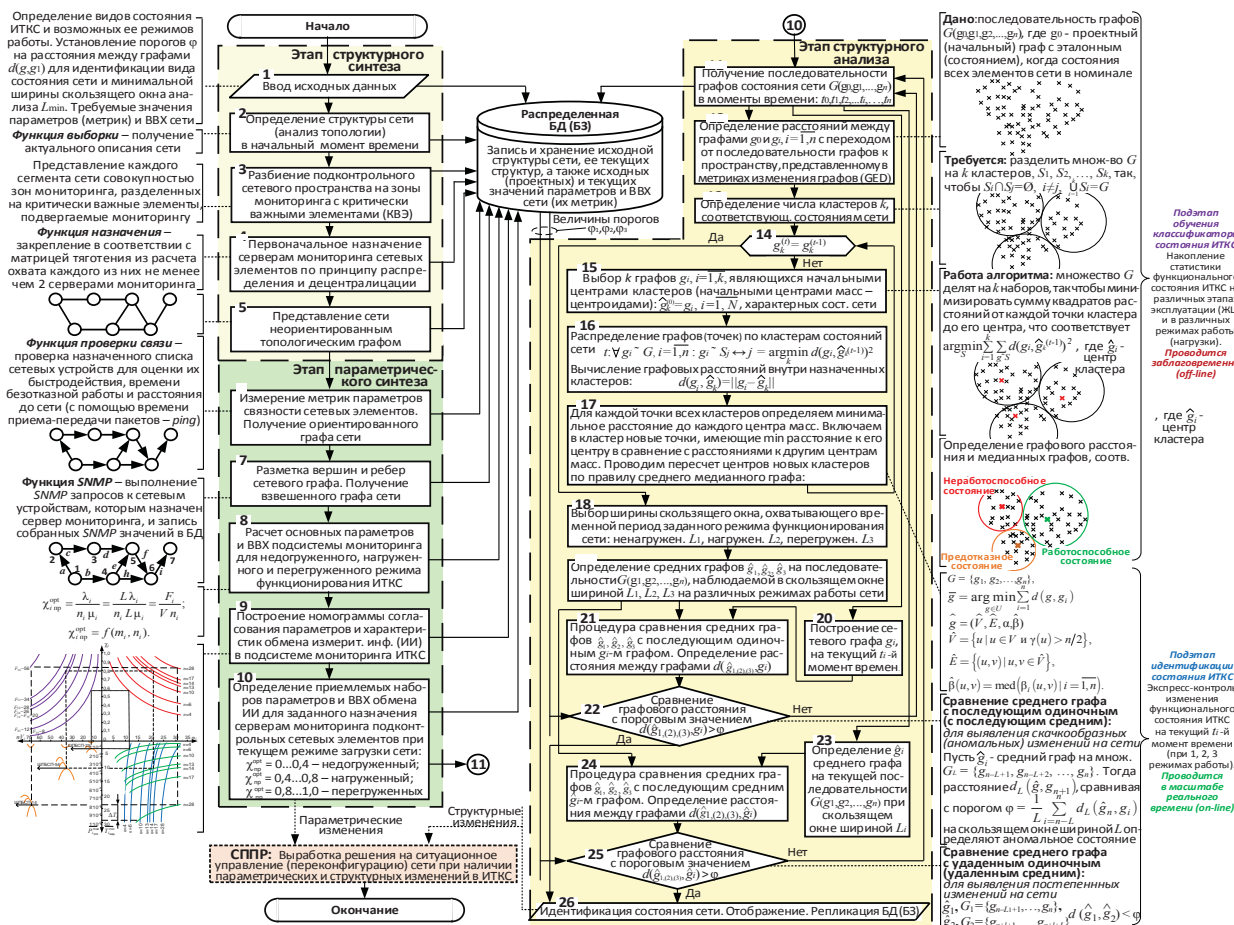


Рис. 10. Блок-схема алгоритма методики синтеза подсистемы интеллектуального мониторинга ИТКС



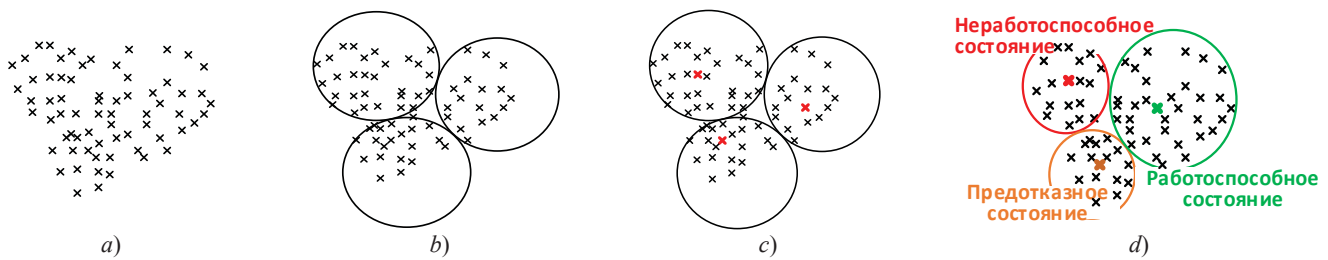


Рис. 11. Процедура модифицированного алгоритма  $k$ -средних при определении состояния сети по их графам

**Этап структурного анализа** состоит из подэтапа обучения классификатора (построенного по модифицированной процедуре алгоритма  $k$ -среднего) и подэтапа непосредственно идентификации состояния сети:

на шаге 11 получают последовательность графов состояния сети  $G(g_0, g_1, g_2, \dots, g_i, \dots, g_n)$  в моменты времени:  $t_0, t_1, t_2, \dots, t_i, \dots, t_n$ , где  $g_0$  начальный (проектный) граф в момент времени  $t_0$  с эталонным (состоянием), когда состояния всех элементов сети (их параметров) находятся в номинальных значениях. Обычная процедура обучения классификатора предполагает, что в качестве исходных данных для идентификации нормального и аномальных состояний сети используются облака данных как неупорядоченные наборы данных, не привязанные к какой-либо из шкал измерений. Однако в отличие от процедуры TDA (Topology Date Analysis) [22, 23], применяемой для анализа временных рядов метрик сетевых элементов, в предлагаемом алгоритме облако данных представляют в виде множества точек в заданном топологическом пространстве метрик графов, описывающих состояния ИТКС во времени. А поскольку в данном алгоритме исходные данные представлены сетевыми графами, то последовательность графов сети  $G$  преобразуется в облако точек, где каждому графу, описываемому графовым расстоянием от графа  $g_0$ , ставится в соответствие точка в облаке данных (рис. 11 а).

на шаге 12 определяют расстояния между графами  $g_0$  и  $g_i, i = \overline{1, n}$  с переходом от последовательности графов к пространству, представленному в метриках изменения (редактирования) графа (graph edit distance, GED): замена метки дуги  $\rightarrow$  изменение состояния канала связи; вставка узла  $\rightarrow$  восстановление (наращивание) узлов сети; вставка дуги  $\rightarrow$  восстановление (добавление) канала связи; удаление узла  $\rightarrow$  отказ узла (деградация сети); удаление дуги  $\rightarrow$  отказ канала (нарушение связности – деградация сети);

на шаге 13 на множестве  $G$  определяют кластеры  $k$  по видам состояния сети  $S_1, S_2, \dots, S_k, S_i \cap S_j = \emptyset, i \neq j$ . Одной из особенностей алгоритма  $k$ -средних является заранее определяемое число кластеров. Для мониторинга сетевых инфраструктур, как правило, в конечной интерпретации оператора подсистемы мониторинга таких состояний всего два «работоспособное состояние («норма») – сеть выполняет свои функции и неработоспособное состояние («авария»), или блокировка сети). С целью недопущения внезапного перехода сети в аварийное состояние, также особый интерес представляет «предотказное состояние», введенное ГОСТ 27.002-2015 и характеризующее повышенным риском отказа ОК, возникающего как в результате внутренних процессов и причин, так и внешних воздействий на сеть в процессе ее функционирования.

В соответствии с международной классификацией (Рек. ITU-T M.3703) «предотказное состояние» соотносится с «критическому». В связи с изложенным, на шаге 13 произвольно определяют на облаке точек три кластера, которые в последующем, после завершения схождения алгоритма  $k$ -средних, будут соответствовать основным состояниям ИТКС, (рис. 11 б).

на шаге 14 проверяют условие прекращения процедуры обучения классификатора  $g_k^{(t)} = g_k^{(t-1)}$ , когда центры масс кластеров (медианные графы) на текущем временном отсчете ( $t$ ) не отличаются от предыдущего ( $t-1$ );

на шаге 15 на заданных при реализации шага 13 кластерах графов выбирают  $k$  средних графов  $g_i, i = \overline{1, k}$ , являющихся начальными центрами кластеров (центрами масс – центроидами) путем процедуры минимизации суммы квадратов расстояний от каждой точки заданного кластера до его центра (рис. 11 с);

на шаге 16 осуществляют перераспределение всех точек графов по кластерам, соответствующим тому или иному состоянию сети путем определения расстояния до центров масс (полученных на шаге 15) от каждого из наблюдаемых графов (рис. 11 d). Если окажется, что рассматриваемый граф ближе к медианному графу (тяготеет к нему), описывающему первое (нормальное) состояние сети – «1», следовательно состояние данного графа имеет такое же состояние, как и граф с центром «1». Если рассматриваемый граф ближе к медианному графу, описывающего состояние «2», то состояние этого графа имеет такое же состояние, как и граф с центром «2», и т. д.

на шаге 17 по выражению (7) проводят пересчет центров вновь сформированных кластеров по правилу среднего медианного графа по всем графам кластера, после чего итерационную процедуру повторяют по шагу 14. Как отмечалось ранее, в динамической системе, к которой относят и распределенные ИТКС, состояние сети постоянно изменяется. Например, выход из строя узла сети (вершины графа) или канала связи (ребра графа) влечет за собой перемаршрутизацию, направленную на восстановление функционального состояния сети. Поэтому с течением времени граф будет претерпевать изменения, в связи с чем на каждом временном интервале мониторинга сети необходима итерация: по определению новых кластеров ее состояния в следующий момент времени  $t+1$ ; назначению центров масс (медианных графов), соответствующих видам состояния сети; определению расстояния наблюдаемого графа до центров масс медианных графов; сравнению вычисленных расстояний и по их минимуму – идентификация вида состояния сети. При этом итерационная процедура повторяется до момента времени, когда рассматриваемый граф не окажется ближе к центру

кластера «2» графа, имеющему «предотказное состояние», или к центру кластера «3» графа, имеющего состояние «авария», или к центру кластера «1» графа с состоянием «норма».

Таким образом, при выполнении условия шага 14, когда центроиды кластеров не перемещаются в графовом пространстве  $g_k^{(i)} = g_k^{(i-1)}$ , итерационные процедуры кластеризации вида состояния прекращают. Фактически подэтап обучения классификатора состояния ИТКС проводится заблаговременно (offline), как правило в период опытной эксплуатации, но накопление статистики функционального состояния ИТКС (дообучение) может осуществляться на разных этапах эксплуатации (ЖЦ) и в различных режимах работы сети.

на шаге 18 осуществляют выбор ширины скользящего окна, охватывающих временные периоды основных (заданных) режимов функционирования сети: ненагруженный  $L_1$ , нагруженный  $L_2$ , перегруженный  $L_3$ ;

на шаге 19 определяют средние (медианные) графы на последовательностях  $G(g_1, g_2, \dots, g_n)$ , наблюдаемых в скользящих окнах шириной  $L_1, L_2, L_3$  при различных режимах работы сети, что необходимо для дальнейшего уточнения состояния сети «работоспособное», «предотказное», «неработоспособное», путем сравнения с текущим  $g$ ;

на шагах 20, 21, 22 для выявления скачкообразных (аномальных) изменений на сети осуществляют сравнение среднего графа, рассчитанного в скользящих окнах шириной  $L_1, L_2, L_3$  с последующим одиночным либо (с последующим средним) по процедурам, описанным в п. 2, рис. 4 и 5;

на шагах 23, 24, 25 для выявления для выявления постепенных изменений на сети осуществляют сравнение среднего графа, рассчитанного в скользящих окнах шириной  $L_1, L_2, L_3$  с удаленным одиночным (удаленным средним) по процедурам, описанным в п. 2, рис. 6 и 7;

на шаге 26 осуществляют идентификацию состояния сети и репликацию (обновление) БД (БЗ). При этом компонент интеллектуальной обработки (рис. 8) транслирует на компонент отображения сигнал о виде технического состояния ИТКС в интересах оператора СППР или автоматизированной системы управления сетью.

Процесс выработки решения на ситуационное управление (переконфигурацию) сети системой СППР при наличии параметрических и структурных изменений в ИТКС выходит за рамки данного исследования.

Таким образом, рассмотренная процедура оценки состояния сети на основе измерения расстояния графов и модификации алгоритма  $k$ -средних является вероятностной версией  $EM$ -алгоритма, рассмотренного [22].

## Заключение

Изложенный в методике подход к синтезу подсистемы мониторинга ИТКС позволил сформулировать следующие основные выводы, направленные на повышение эффективности СППР ситуационного центра Министерства транспорта РФ за счет сопряжения формируемой его подсистемы интеллектуального мониторинга с сетевыми элементами гетерогенного межведомственного подконтрольного пространства:

анализ этапов развития современных сетевых инфраструктур, а также переход от гомогенных к гетерогенным межведомственным ИТКС показал непрерывный, экспоненциальный рост контролируемого пространства, порождаемый увеличением территориальной распределенности и неоднородности телекоммуникационных систем в процессе их функционирования, что предполагает соответствующий охват средствами интеллектуального мониторинга наблюдаемых сетевых элементов;

для сокращения (редуцирования) контролируемого пространства, характеризуемого топологической и пространственно-временной неоднородностью, показано, что любая развивающаяся система связи, с учетом свойств эволюционного развития, динамичности структуры и вариативности данных аспектов, может быть представлена как совокупность зон мониторинга, разделенных на КВЭ, масштабируемые на любом этапе развития ИТКС. Редуцирование контролируемого пространства позволяет рассматривать концептуальную модель интеллектуального мониторинга для нахождения соответствия эксплуатационных параметров сетевых элементов установленным требованиям, объединяющей концепции измерений, анализа и тестирования, что позволит обеспечить управление ИТКС, ее элементами, а также реконфигурацию сети, своевременно обнаруживать и устранять неисправности и, в целом, способствует обеспечению устойчивого ее функционирования;

структуризация контролируемого пространства терминами «зона мониторинга», «критически важный элемент» и «классы состояния» составляют основу новых методов интеллектуального мониторинга, являющихся «нечувствительными» к свойству постоянного совершенствования (эволюционирования) и неоднородности гетерогенных сетевых инфраструктур. При этом в ходе проведенного структурного синтеза подсистемы интеллектуального мониторинга ИТКС на основе гиперграфа топологической взаимосвязи зон мониторинга ведомства построена структура подсистемы мониторинга для последующего параметрического синтеза;

полученные в ходе параметрического синтеза подсистемы мониторинга ИТКС значения  $\chi_{i\ pr}^{opt}$  наряду с формулой (25) позволяют рассчитать пропускные способности каналов ТИ-ТС  $V_i$  и нужный объем буферной памяти  $m_i$  при известной топологии (этап структурного синтеза) и заданной матрице тяготения потоков измерительной информации  $\|F_{ij}\|$  от сенсоров сетевых элементов ИТКС к серверу мониторинга ситуационного центра, обеспечивающие среднее минимальное время доставки измерительной информации и значение максимальной вероятности отказа в обслуживании её пакетов в допустимых пределах.

Таким образом, последовательно проведенные этап структурного синтеза подсистемы мониторинга ИТКС, а также этап ее параметрического синтеза и этап структурного анализа с использованием процедур измерения графовых расстояний и метода  $k$ -средних, позволяют не только идентифицировать вид состояния сети, но и обоснованно, с использованием инструментальных методов расчета основных параметров и ВВХ переконфигурировать сеть для недопущения её перехода в состояние блокировки (неработоспособное состояние).

## Литература

1. *Зацаринный А.А., Сучков А.П.* Системотехнические подходы к созданию системы поддержки принятия решений на основе ситуационного анализа // Информатика и ее применение. 2016. Т. 10. № 4. С. 105-113.
2. *Будко П.А., Кулешов И.А., Курносков В.И., Мирошников В.И.* Инфокоммуникационные сети: энциклопедия. Кн. 4. Гетерогенные сети связи: принципы построения, методы синтеза, эффективность, цена, качество / под ред. проф. В. И. Мирошникова. М.: Наука, 2020. 683 с.
3. *Аллакин В.В.* Формирование сервера мониторинга функциональной безопасности информационно-телекоммуникационной сети общего пользования на основе оценки SRE-метрики // Техника средств связи. 2021. № 1 (153). С. 77-85.
4. *Будко П.А., Рисман О.В.* Многоуровневый синтез информационно-телекоммуникационных систем. Математические модели и методы оптимизации. СПб.: ВАС, 2011. 476 с.
5. *Легков К.Е., Буренин А.Н.* Модели и методы оперативного мониторинга информационных подсистем перспективных автоматизированных систем управления // Информатика и космос. 2016. № 4. С. 46-60.
6. *Легков К.Е.* Модели и методы мониторинга параметров, характеризующих состояние инфокоммуникационной системы специального назначения // Т-Сопт: Телекоммуникации и транспорт. 2016. Т. 10. № 1. С. 11-18.
7. *Сторожук М.* Использование систем мониторинга сетей для обеспечения работы критически важных приложений // Первая миля. 2021. № 1. С. 40-44.
8. *Бакланов И.Г.* Оправдание OSS. М.: Издательские решения, 2016. 131 с.
9. Report to the Nations on Occupational Fraud and Abuse. URL: <https://www.acfe.com/rftn/docs/2014-report-to-nations.pdf> (дата обращения: 08.08.2021).
10. *Будко Н.П.* Сокращение объема измерительной информации на основе интеллектуального подхода к построению системы мониторинга информационно-телекоммуникационной системы // Техника средств связи. 2021. № 1 (153). С. 86-97.
11. Патент РФ на изобретение № 2450335. МПК G06F 15/00, G05B 23/02. Способ распределенного контроля и адаптивного управления многоуровневой системой и устройство для его осуществления. / Будко Н.П.,

- Будко П.А., Винограденко А.М., Дорошенко Г.П., Рожнов А.В., Минев В.В., Мухин А.В.; заявл. 11.07.2011; опубл. 10.05.2012, Бюл. № 13.
12. *Bunke H., Dickinson P.J., Kraetzl M., Wallis W.D.* A Graph-Theoretic Approach to Enterprise Network Dynamics. Basel: Birkhauser, 2007. 226 p.
13. *Shoubridge P., Kraetzl M., Wallis W.D., Bunke H.* Detection of abnormal change in time series of graphs. Journal of Interconnection Networks, 3(1&2): 85-101, 2002.
14. *Wallis W.D., Shoubridge P.J., Kraetzl M., Ray D.* Graph distances using graph union. Pattern Recognition Letters, 22:701-704, 2001.
15. *Parkes D.D., Wallis W.D.* Graph Theory and the Study of Activity Structure. Timing Space and Spacing Time, vol. 2: Human Activity and Time Geography. Edward Arnold, London, 1978.
16. *Uneyama S.* An eigendecomposition approach to weighted graph matching problems. IEEE Transactions on Pattern Recognition and Machine Intelligence, 10(5):695-703, September 1988.
17. *Цветкович Д., Дуб М., Захс Х.* Спектры графов: теория и применение. Киев: Наукова думка, 1984. 383 с.
18. *Мизин И.А., Богатырев В.А., Кулешов А.П.* Сети коммутации пакетов / под ред. В.С. Семенкина. М.: Радио и связь, 1986. 408 с.
19. *Каретников В.В., Будко Н.П., Аллакин В.В.* Синтез подсистемы интеллектуального мониторинга информационно-телекоммуникационной сети ведомственного ситуационного центра // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2021. № 3. С. 64-81. DOI: 10.24143/2072-9502-2021-3-64-81.
20. *Вентцель Е.С.* Исследование операций. М.: Наука, 1989. 275 с.
21. *Бильгаева Л.П., Самбялов З.Г.* Оценка качества алгоритмов кластеризации. Улан-Удэ: Вестник Восточно-Сибирского государственного университета технологий и управления, 2013. Вып. 6. С. 53-60.
22. *Аллакин В.В., Будко Н.П., Васильев Н.В.* Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Системы управления, связи и безопасности. 2021. № 4. С. 125-227. DOI: 10.24412/2410-9916-2021-4-125-227.
23. *Нашивичников Н.В., Пустарнаков В.Ф.* Топологические методы анализа в системах поведенческой аналитики // Вопросы кибербезопасности. 2021. № 2. С. 26-36.

## THE METHOD OF SYNTHESIS OF THE SUBSYSTEM OF INTELLIGENT MONITORING OF THE INFORMATION AND TELECOMMUNICATIONS NETWORK OF THE SITUATION CENTER

**NIKITA P. BUDKO,**  
St. Petersburg, Russia, budko62@mail.ru

**KEYWORDS:** *k-means algorithm, identification of the type of network state, median graph, monitoring subsystem, parametric synthesis stage, structural analysis stage, structural synthesis stage.*

### ABSTRACT

**Introduction:** in accordance with the task of forming a system of distributed situational centers of public authorities, it is necessary to interface heterogeneous segments of the department's information and telecommunications networks into a geographically distributed infrastructure with the construction of a subsystem for monitoring the state of its elements on it. **The purpose of the study:** based on the use of basic concepts of structural synthesis methods, structural analysis of network infrastructures, as well as parametric synthesis procedures, to develop a methodology for the synthesis of a new generation monitoring subsystem based on intelligent methods for identifying the state of the network. **Results:** the structuring of the controlled space by the terms "monitoring zone", "critical element", "state classes "form the basis of new methods of intelligent monitoring that are" insensitive " to the properties of the constant evolution of network infrastructures. The proposed method of synthesis of the intelligent monitoring subsystem consists of sequentially performed stages of structural synthesis, parametric synthe-

sis and structural analysis of the network. **Practical significance:** the successive stages of the methodology using graph distance measurement procedures and the modified k-means algorithm allow not only to identify the type of network state, but also to reasonably, using instrumental calculation methods, present in the interests of the decision support system sets of acceptable values of the main parameters and probabilistic-temporal characteristics of the monitoring subsystem for subsequent reconfiguration of the network and preventing its transition to an inoperable state. **Discussion:** the modification of the k-means algorithm proposed in the study differs in that in the classical algorithm, work is carried out on points of Euclidean space, and in the proposed method we are talking about a graph space with metrics in the form of graph distances, while data clouds are used as initial data for classification in the k-means algorithm as disordered data sets that are not tied to any of the measurement scales, and in the proposed algorithm, the data cloud is represented by a set of graphs in a given topological space of graph metrics, describing the state of the network in time.



REFERENCES

1. Zatsarinny A.A., Suchkov A.P. (2016). Systems engineering approaches to the establishment of a system for decision support based on situational analysis. *Informatics and applications*. Vol. 10. No. 4. Pp. 105-113. (In Russian)
- Zatsarinny A. A., Shabanov A. P. (2015). *Tekhnologiya informacionnoj podderzhki deyatel'nosti organizacionnyh sistem na osnove situacionnyh centrov* [Technology of information support for the activities of organizational systems based on situational centers]. Moscow: TORUS PRESS. 232 p. (In Russian)
2. Budko P. A., Kuleshov I. A., Kurnosov V. I., Miroshnikov V. I. (2020). *Infokommunikacionnye seti: enciklopediya*. Kn. 4. *Geterogennye seti svyazi: principy postroeniya, metody sinteza, effektivnost', tsena, kachestvo* [Infocommunication networks: an encyclopedia. Book 4. Heterogeneous communication networks: principles of construction, methods of synthesis, efficiency, price, quality]. Moscow: Nauka Publ. 683 p. (In Russian)
3. Allakin V. V. (2021). Formation of a server for monitoring the functional security of a public information and telecommunications network based on the evaluation of SRE metrics. *Means of Communication Equipment*. No. 1 (151). Pp. 77-85. (In Russian)
4. Budko P. A., Risman O. V. (2011). *Mnogourovnevnyj sintez informacionno-telekommunikacionnyh sistem. Matematicheskie modeli i metody optimizacii* [Multilevel synthesis of information and telecommunications systems. Mathematical models and optimization methods]. St. Petersburg: Military Academy of Communications Publ., 476 p. (In Russian)
5. Legkov K. E., Burenin A. N. (2016). Models and methods for monitoring of information subsystems of prospective automated control systems. *Information and Space*. No. 4. Pp.46-60. (in Russian).
6. Legkov K.E. (2016). Models and methods of monitoring parameters characterizing the state of the infocommunication systems a special purpose. *T-Comm*. Vol. 10. No.1, pp. 11-18. (in Russian)
7. Storozhuk M. (2021). *Ispol'zovanie sistem monitoringa setej dlya obespecheniya raboty kriticheski vazhnyh prilozhenij* [The use of network monitoring systems to ensure the operation of critical applications]. *The first mile*. No. 1. pp. 40-44. (In Russian)
8. Baklanov I. G. (2016). *Opravdanie OSS* [Justification of OSS]. Moscow: Publishing solutions. 131 p. (In Russian)
9. Report to the Nations on Occupational Fraud and Abuse. URL: <https://www.acfe.com/rtn/docs/2014-report-to-nations.pdf> (accessed: 06.12.2020).
10. Budko N.P. (2021). Reducing the amount of measurement information based on an intelligent approach to build a monitoring system for an information and telecommunications system. *Means of Communication Equipment*. No. 1 (151). Pp. 86-97. (In Russian)
11. Patent RF 2450335. *Sposob raspredelennogo kontrolya i adaptivnogo upravleniya mnogourovnevoj sistemoj i ustrojstvo dlya ego osushchestvleniya* [A method of distributed control and adaptive control of a multi-level system and a device for its implementation]. Budko N. P., Budko P. A., Vinogradenko A. M., Doroshenko, G. P., Rozhnov A. V., Mineev V. V., Mukhin V. A. Declared 11.07.2011. Published 10.05.2012. Bulletin No. 13. 30 p. (In Russian)
12. Bunke H., Dickinson P. J., Kraetzl M., Wallis W. D. (2007). *A Graph-Theoretic Approach to Enterprise Network Dynamics*. Basel: Birkhauser. 226 p. (In Rus)
13. Shoubridge P., Kraetzl M., Wallis W.D., Bunke H. (2002). Detection of abnormal change in time series of graphs. *Journal of Interconnection Networks*, 3(1&2). Pp. 85-101.
14. Wallis W.D., Shoubridge P.J., Kraetzl M., Ray D. (2001). Graph distances using graph union. *Pattern Recognition Letters*, 22. Pp. 701-704.
15. Parkes D.D., Wallis W.D. (1978). *Graph Theory and the Study of Activity Structure. Timing Space and Spacing Time*, vol. 2: Human Activity and Time Geography. Edward Arnold, London.
16. Umeyama S. (1988). An eigendecomposition approach to weighted graph matching problems. *IEEE Transactions on Pattern Recognition and Machine Intelligence*, 10(5). Pp. 695-703, September 1988.
17. Tsvetkovich D., Dubh M., Sachs H. (1984). *Spektry grafov: teoriya i primenenie* [Graph spectra: theory and application]. Kiev: Naukova dumka Publ. 383 p. (In Russian)
18. Mizin I. A., Bogatyrev V. A., Kuleshov A. P. (1986). *Seti kommutacii paketov* [Packet switching networks]. Moscow: Radio and Communications Publ. 408 p. (In Russian)
19. Karetnikov V. V., Budko N. P., Allakin V. V. (2021). Synthesis of subsystem of intelligent monitoring of information and telecommunication network of departmental situational center. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. No. 3. Pp. 64-81. (In Russian) DOI: 10.24143/2072-9502-2021-3-64-81.
20. Wentzel E. S. (1989). *Issledovanie operacij* [Operations research]. Moscow: Nauka Publ. 275 p. (In Russian)
21. Bilgaeva L. P., Sambyalov Z. G. (2013). *Ocenka kachestva algoritmov klasterizacii* [Evaluation of the quality of clustering algorithms]. Ulan-Ude: *Bulletin East Siberia State University of Technology and Management*. Issue. 6. Pp. 53-60. (In Russian)
22. Allakin V. V., Budko N. P., Vasiliev N. V. (2021). A general approach to the construction of advanced monitoring systems for distributed information and telecommunications networks. *Systems of Control, Communication and Security*. No. 4. Pp. 125-227. (in Rus). DOI: 10.24412/2410-9916-2021-4-125-227. (In Russian)
23. Nashivochnikov N. V., Pustarnakov V. F. (2021). *Topologicheskie metody analiza v sistemah povedencheskoj analitiki* [Topological methods of analysis in behavioral analytics systems]. *Voprosy kiberbezopasnosti*. No. 2. pp. 26-36. (In Russian)

INFORMATION ABOUT AUTHOR:

**Nikita P. Budko**, postgraduate student, Federal State Budgetary Educational Institution of Higher Education "Admiral S. O. Makarov State University of the Sea and River Fleet", St. Petersburg, Russia, budko62@mail.ru

**For citation:** Budko N.P. The method of synthesis of the subsystem of intelligent monitoring of the information and telecommunications network of the situation center. H&ES Reserch. 2021. Vol. 13. No. No 5. P. 38-56. doi: 10.36724/2409-5419-2021-13-5-38-56 (In Rus)





doi: 10.36724/2409-5419-2021-13-5-57-74

# АЛГОРИТМЫ ОЦЕНКИ И КОМПЕНСАЦИИ ДИСПЕРСИОННЫХ ИСКАЖЕНИЙ ШИРОКОПОЛОСНЫХ СИГНАЛОВ ИОНОСФЕРНЫХ РАДИОЛИНИЙ СВЯЗИ

**АДЖЕМОВ**

Сергей Сергеевич<sup>1</sup>

**ЛОБОВ**

Евгений Михайлович<sup>2</sup>

**КАНДАУРОВ**

Николай Александрович<sup>3</sup>

**ЛОБОВА**

Елизавета Олеговна<sup>4</sup>

**ЛИПАТКИН**

Владислав Игоревич<sup>5</sup>

## АННОТАЦИЯ

**Введение:** в настоящее время радиосвязь в декаметровом диапазоне активно используется для осуществления связи в удалённых и труднодоступных регионах мира. Декаметровая связь также является актуальным типом радиосвязи для регионов, претерпевших серьёзные разрушения из-за стихийных бедствий. Актуальность применения декаметровой радиосвязи в вышеописанных случаях связана с тем, что данная технология может предложить надёжные и дешёвые решения. Вторая область применения декаметровой радиосвязи – это связь в Арктике и Антарктике. **Практическая значимость:** при приёме сигналов с расширенным спектром возникает необходимость учёта влияния частотной дисперсии ионосферного канала, так как она приводит к существенным искажениям полезного сигнала и снижению качества связи в целом. Актуальной задачей является оценка параметров частотной дисперсии ионосферного канала и разработка алгоритмов и устройств компенсации дисперсионных искажений широкополосных сигналов. **Обсуждение:** в статье приведены алгоритмы оценки и компенсации дисперсионных искажений широкополосных сигналов декаметровых радиолиний связи. Рассматриваются методы оценки наклона дисперсионной характеристики, а именно, оценка методом максимального правдоподобия (МП), оценка методом деления сигнала на подполосы, совместная оценка наклона дисперсионной характеристики с другими параметрами широкополосного сигнала. Предлагаются алгоритмы компенсации дисперсионных искажений широкополосных сигналов. Первый метод: компенсация во время обнаружения сигнала согласованным фильтром. Второй метод: компенсация с помощью банков цифровых фильтров. Третий метод: обработка сигнала следящим компенсатором. Приведены результаты натурных экспериментов по компенсации дисперсионных искажений у широкополосного сигнала на односкачковой трассе протяженностью около 2900 км.

## Сведения об авторах:

<sup>1</sup> д.т.н., профессор, МТУСИ, Москва, Россия

<sup>2</sup> к.т.н., доц., зав. НИЛ-4806 НИЧ МТУСИ, Москва, Россия, lobov@srd.mtuci.ru

<sup>3</sup> кк.т.н., зав. НИЛ-4808 НИЧ МТУСИ, Москва, Россия, jet1992@yandex.ru

<sup>4</sup> м.н.с. НИЛ-4803 НИЧ МТУСИ, Москва, Россия, lizabeth2@mail.ru

<sup>5</sup> инженер 1-й категории НИЧ МТУСИ, Москва, Россия, lipatkin.24@gmail.com

**КЛЮЧЕВЫЕ СЛОВА:** ионосфера, широкополосная связь, дисперсионные искажения, оценка параметров сигналов, компенсация

**Для цитирования:** Аджемов С.С., Лобов Е.М., Кандауров Н.А., Лобова Е.О., Липаткин В.И. Алгоритмы оценки и компенсации дисперсионных искажений широкополосных сигналов ионосферных радиолиний связи // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 57-74. doi: 10.36724/2409-5419-2021-13-5-57-74

## Введение

В настоящее время радиосвязь в декаметровом диапазоне активно используется для осуществления связи в удалённых и труднодоступных регионах мира. Декаметровая связь также является актуальным типом радиосвязи для регионов, претерпевших серьёзные разрушения из-за стихийных бедствий. Актуальность применения декаметровой радиосвязи в вышеописанных случаях связана с тем, что данная технология может предложить надёжные и дешёвые решения. Вторая область применения декаметровой радиосвязи – это связь в Арктике и Антарктике. Так как в данных регионах активно развита научная деятельность, связанная с биологическими и геофизическими исследованиями, то есть необходимость передачи информации с сенсоров, расположенных в разных частях южного континента, на полярные станции или на другие материка. Связь в декаметровом диапазоне в Арктике и Антарктике применяется в качестве альтернативы спутниковой связи по той причине, что спутники на геостационарной орбите не видны с полюсов. В последнее время установилась тенденция использования систем связи коротковолнового диапазона с повышением скорости передачи информации (или наоборот применению на вторичной основе) за счёт увеличения используемой полосы частот до 400 кГц и выше [1-8].

Актуальность декаметровой радиосвязи и новые вызовы, возникающие именно при переходе к широкополосным каналам, требуют совершенствования всех устройств и алгоритмов, входящих в систему радиосвязи. В частности, исследования многими авторами ведутся по ряду направлений:

- разработка высокоэффективных усилителей мощности и устройств, согласующих тракт передатчика с антенно-фидерными устройствами [9-15];

- разработка новых моделей широкополосного ионосферного канала и моделей, в том числе учитывающих ионосферные возмущения [16-19];

- разработка новых сигнально-кодовых конструкций, адаптированных к широкополосным эффектам ионосферы Земли [**Ошибка! Источник ссылки не найден.**, 5-8, 20-31];

- разработка алгоритмов приёма сигналов в условиях наличия множества узкополосных помех [32-35];

- разработка алгоритмов многоантенной передачи и многоантенного приема (MIMO), а также алгоритмов, учитывающих эффекты поляризации [36-42];

- разработка алгоритмов оценки и компенсации искажений сигнала в широкополосном ионосферном канале, в том числе специфических дисперсионных искажений [43-54] и с применением вычислительно эффективных схем [55-59].

При приёме сигналов с расширенным спектром возникает необходимость учёта влияния частотной дисперсии ионосферного канала, так как она приводит к существенным искажениям полезного сигнала и снижению качества связи в целом. С учётом изложенного, актуальной задачей является оценка параметров частотной дисперсии ионосферного канала и разработка алгоритмов и устройств компенсации дисперсионных искажений широкополосных сигналов [44, 45, 47]. В широкополосных системах передачи данных для

обработки сигналов уже длительное время активно используются цифровые банки фильтров [63]. В том числе, в работах [47, 48, 55] были получены алгоритмы компенсации дисперсионных искажений, основанных на «выравнивании» задержек и компенсации фазовых сдвигов в отдельных подканалах банка фильтров. Данная статья посвящена аналитическому обзору полученных теоретических и экспериментальных результатов оценки и компенсации дисперсионных искажений широкополосных сигналов, полученных коллективом МТУСИ.

## Дисперсионные искажения и модель канала

Частотная дисперсия среды распространения ЭМ волн (в т.ч. ионосферы) – зависимость коэффициента диэлектрической проницаемости от частоты, распространяющейся в ней ЭМ волны. При распространении широкополосных сигналов по наклонным траекториям в ионосфере, отдельные группы гармоник из состава спектра сигнала распространяются по разным криволинейным траекториям, с различными высотами точек поворота (см. рис. 1). Указанные дисперсионные искажения широкополосных сигналов приводят к уменьшению по уровню и размытию во времени отклика согласованного фильтра на приемной стороне. При этом уменьшается вероятность обнаружения сигнала, точность измерения его задержки распространения, что влияет на качество синхронизации, и уменьшается помехоустойчивость передачи информации.

В качестве модели канала с частотной дисперсией принята модель канала с линейной зависимостью групповой задержки сигнала от центральной частоты (линейная дисперсионная характеристика с наклоном  $s$ , см. рисунок . 2) [16]. Передаточная функция ионосферного канала для  $i$ -й многолучевой компоненты

$$\dot{H}_i(f) = \int_{-\infty}^{\infty} \dot{h}_i(t) e^{-j2\pi ft} dt = e^{-j(\varphi_i(f_p) + 2\pi\tau_i(f_p)(f-f_p) + \pi s_i(f-f_p)^2)}$$

$$f \in \left[ f_p - \frac{\Delta f}{2}, f_p + \frac{\Delta f}{2} \right]$$

$$-\varphi_i(f) \approx -\varphi_i(f_p) - 2\pi\tau_i(f_p)(f-f_p) - \pi s_i(f-f_p)^2,$$

$$\tau_i(f) \approx \tau_i(f_p) + s_i(f-f_p)$$

$f_p$  – центральная частота спектра сигнала,  $\Delta f$  – ширина спектра сигнала,  $\tau_i(f_p)$  – групповая задержка сигнала на центральной частоте,  $s_i$  – наклон дисперсионной характеристики (ДХ)  $i$ -го луча, обуславливающая дисперсионные искажения. Фазочастотная характеристика канала описывается квадратичной зависимостью от частоты, а групповая задержка распространения – линейной с наклоном  $s$  мкс/МГц.

Для простоты ограничимся лишь квадратичным членом ФЧХ:

$$\dot{H}_i(f) = e^{-j\pi s f^2} = e^{-j\pi s \left(\frac{\omega}{2\pi}\right)^2}. \quad (1)$$

Будем рассматривать все сигналы с позиции их комплексных огибающих, т.е. при нулевой центральной частоте ( $f_p = 0$ ).

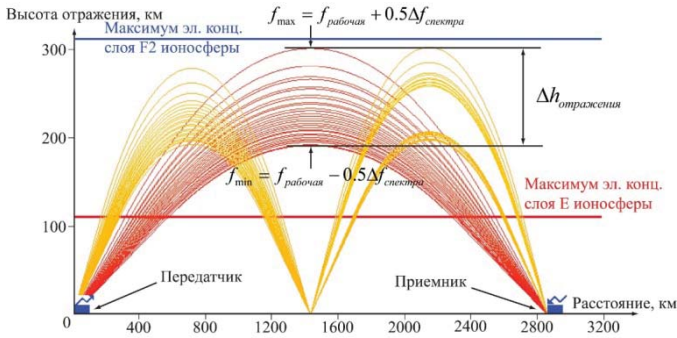


Рис. 1. Траектории распространения отдельных групп гармоник из состава спектра широкополосного сигнала

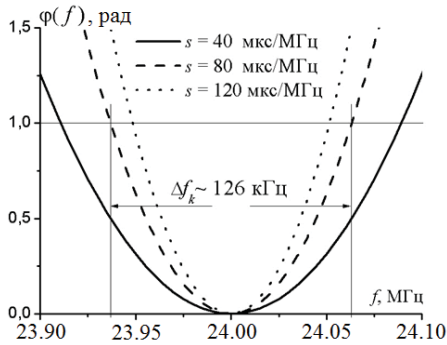
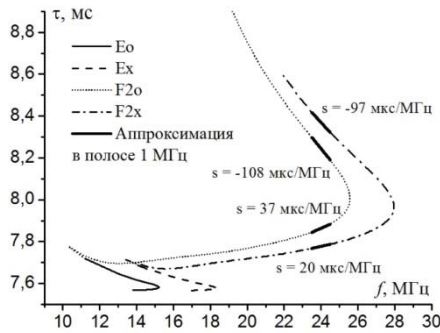


Рис. 2. Расчетные дисперсионные кривые (слева), квадратичная часть ФЧХ канала (справа)

### Методы оценки наклона дисперсионной характеристики

Пусть на выходе цифрового квадратурного демодулятора наблюдается выборка значений случайного процесса  $\dot{y}_i$ , являющегося суммой полезного сигнала  $\dot{x}_i(s)$ , искаженного частотной дисперсией, с некоторым сдвигом по фазе  $\varphi_0$  и шумовой составляющей  $\dot{n}_i$ :

$$\dot{y}_i = \dot{x}_i(s) e^{j\varphi_0} + \dot{n}_i, \quad i = 0, 1, \dots, N_s - 1,$$

где  $\dot{n}_i = n_{\text{Re}i} + j n_{\text{Im}i}$  – комплексные гауссовские величины, вещественная и мнимая часть которых центрированы, имеют одинаковую дисперсию  $\sigma_{\text{ш}}^2$  и независимы между собой.

Алгоритм формирования искаженного частотной дисперсией сигнала  $\dot{x}_i(s)$  на основе излученного сигнала  $\dot{x}_i$  известен:

$$\dot{x}_i(s) = \frac{1}{N_s} \sum_{k=-N_s/2}^{N_s/2-1} \dot{X}_k \dot{H}_k e^{j \frac{2\pi i k s}{N_s}}, \quad \dot{H}_k = e^{-j\pi s f_k^2},$$

где  $\dot{X}_k$  – коэффициенты ДПФ известного излученного сигнала  $\dot{x}_i$ ;  $i$  – номер отсчета;  $\dot{H}_k$  – значения частотной характеристики в дискретных точках  $f_k$ , Гц;  $\dot{H}_k$  – значения передаточной функции канала в точках  $f_k$ , Гц;  $s$  – наклон ДХ.

### Оценка методом максимального правдоподобия (МП)

Алгоритм нахождения оценки постоянного параметра с помощью метода МП известен и здесь приводиться не будет [45].

Дисперсия такой точечной оценки  $\hat{s}$  может быть найдена по уточненным выражениям в приближении высоких отношений сигнал/шум (ОСШ) по формулам [44, 45]:

$$D(\hat{s} / \mathbf{y}) = -\frac{1}{\rho^2} \left[ \frac{d^2 S(s, \hat{s})}{ds^2} \right]^{-1} \left[ 1 + \frac{1}{\rho^2} \frac{d^4 S(s, \hat{s})}{ds^4} \left( \frac{d^2 S(s, \hat{s})}{ds^2} \right)^{-2} \right]_{\hat{s}=\hat{s}},$$

если начальная фаза сигнала  $\varphi_0$  известна;

$$D(\hat{s} / \mathbf{y}) = -\frac{1}{\rho^2} \left[ \frac{d^2 G(s, \hat{s})}{ds^2} \right]^{-1} \left[ 1 + \frac{1}{\rho^2} \left( 1 + \frac{d^4 G(s, \hat{s})}{ds^4} \left( \frac{d^2 G(s, \hat{s})}{ds^2} \right)^{-2} \right) \right]_{\hat{s}=\hat{s}},$$

если начальная фаза сигнала  $\varphi_0$  неизвестна и является случайной равномерно распределенной на интервале  $[0, 2\pi]$  величиной, где  $\rho^2 = \frac{2E}{N_0}$  – ОСШ;  $E = \sum_{i=0}^{N_s-1} |\dot{x}_i|^2 = \frac{1}{N_s} \sum_{k=-N_s/2}^{N_s/2-1} |\dot{X}_k|^2$ ;  $\mathbf{y}$  – вектор наблюдаемой выборки. Функции  $S(s, \hat{s})$  и  $G(s, \hat{s})$  – нормированные сигнальные части статистики на выходе коррелятора. В нашем случае:

$$S(s, \hat{s}) = E^{-1} \text{Re} \left( \sum_{i=0}^{N_s-1} \dot{x}_i(s) \dot{x}_i^*(\hat{s}) \right) = E^{-1} \text{Re} \left( \sum_{k=-N_s/2}^{N_s/2-1} |\dot{X}_k|^2 e^{-j\pi f_k^2 (s-\hat{s})} \right);$$

$$G(s, \hat{s}) = E^{-1} \left| \sum_{i=0}^{N_s-1} \dot{x}_i(s) \dot{x}_i^*(\hat{s}) \right| = E^{-1} \left| \sum_{k=-N_s/2}^{N_s/2-1} |\dot{X}_k|^2 e^{-j\pi f_k^2 (s-\hat{s})} \right|.$$

Можно показать, что дисперсия оценки определится следующими выражениями соответственно при известной и случайной начальной фазе:

$$\sigma_s^2 = \frac{1}{2E/N_0} \frac{1}{F_2} \left[ 1 + \frac{1}{2E/N_0} \frac{F_4}{F_2^2} \right]; \quad (2)$$

и

$$\sigma_s^2 = \frac{1}{2E/N_0} \frac{1}{G_2} \left[ 1 + \frac{1}{2E/N_0} \left[ 1 + \frac{G_4}{G_2^2} \right] \right], \quad (3)$$

где  $F_u = (N_s E)^{-1} \sum_{k=-N_s/2}^{N_s/2-1} (\pi f_k^2)^u |\dot{X}_k|^2$ ;  $G_2 = F_1^2 - EF_2$ ;  
 $G_4 = 3F_2^2 + EF_4 - 4F_1F_3 - 3G_2^2$ .

Дисперсия оценки не зависит от истинного значения параметра  $s$ , а зависит только от ОСШ  $E/N_0$  и спектра сигнала  $\dot{X}_k$ . При использовании широкополосных сигналов с равномерным спектром ширины  $\Delta f$  формулы преобразовываются к виду:

$$\sigma_s^2 = \frac{40}{\pi^2 \Delta f^4 (E/N_0)} \left[ 1 + \frac{25}{18} \frac{1}{E/N_0} \right] \text{ и}$$

$$\sigma_s^2 = \frac{90}{\pi^2 \Delta f^4 (E/N_0)} \left[ 1 + \frac{11}{7} \frac{1}{E/N_0} \right] \quad (4)$$

Как следует из (4), дисперсия оценки параметра  $s$  обратно пропорциональна четвертой степени ширины спектра сигнала  $\Delta f$ . Действительно, чем шире спектр сигнала, тем он чувствительнее к изменениям  $s$ , так как сильнее искажается в результате дисперсионных свойств ионосферы. Именно это обуславливает более точную оценку параметра  $s$  сигналами с широким спектром.

Отсчеты сигнально шумовой смеси подавались на согласованный фильтр (СФ), где опорный сигнал каждого был пропущен через фильтр с импульсной характеристикой, учитывающей дисперсионные искажения с наклоном ДХ  $s_i = i \cdot \Delta s, i = 0 \dots N_{сф} - 1$ , где  $\Delta s$  – шаг наклона ДХ,  $N_{сф}$  – количество согласованных фильтров. Затем оценивался отклик и выбирался максимальный среди всех используемых  $s_i$ .

Сравнение расчетных кривых СКО  $\sigma_s$  с выборочными значениями, полученными в результате вычислительного эксперимента, представлено на рисунке 3.

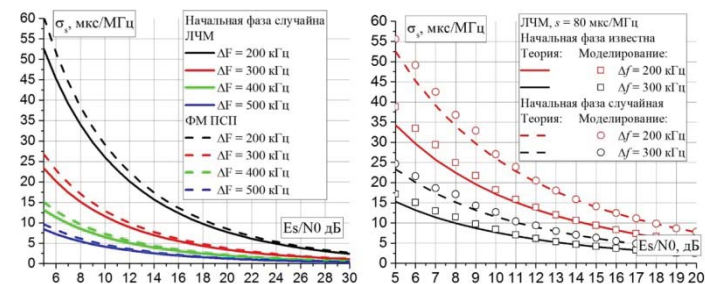


Рис. 3. Кривые СКО оценки параметра  $s$

В качестве зондирующего сигнала использовались: сигнал с линейной частотной модуляцией (девиация частоты 200-500 кГц), фазоманипулированный сигнал на базе кода Голда (ФМ ПСП) длиной 2047 символов; скорость передачи символов ПСП составила 200-500 кбод; форма символов задавалась формирующим фильтром с АЧХ типа корень квадратный из приподнятого косинуса; коэффициент сгла-

живания 0,1. Реальное значение  $s = 80$  мкс/МГц, что соответствует коротким односкачковым трассам [16]. Видно, что при высоких ОСШ (больше 15 дБ) расчетные кривые и экспериментальные значения находятся в хорошем согласии, а при ОСШ < 10 дБ наблюдается их существенное расхождение, которое объясняется тем, что выражения для дисперсии получены в предположении высоких ОСШ.

#### Оценка методом деления сигнала на подполосы

В предлагаемом методе рассматривается широкополосный сигнал как совокупность  $N$  неперекрывающихся по спектру сигналов с одинаковой шириной спектра  $\Delta f_n = \Delta f / N$ , которые будем называть подполосами (см. рис. 4). Количество подполос выбирается таким образом, чтобы влиянием частотной дисперсии на сигнал в рамках одной подполосы можно было пренебречь (см. рис. 5).

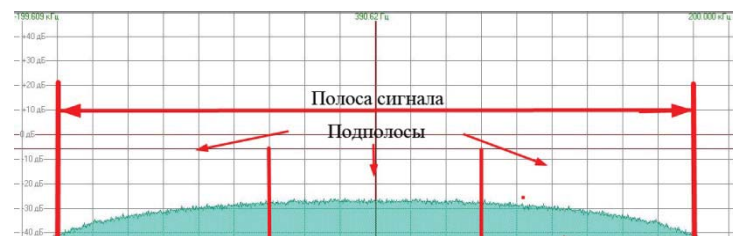


Рис. 4. Подполосы сигнала

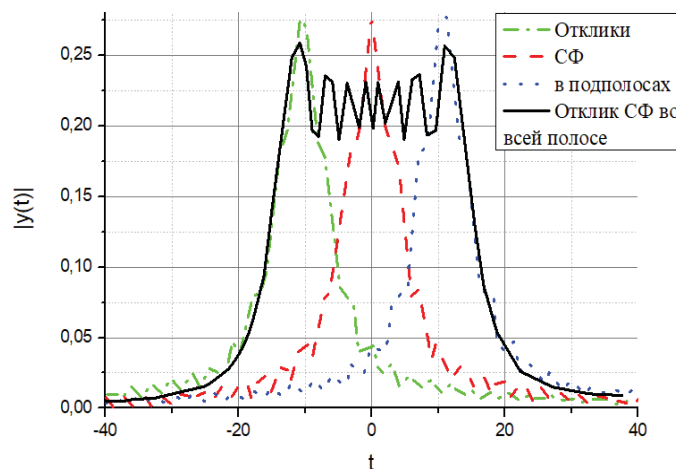


Рис. 5. Отклики согласованного фильтра на подполосы

Изменение групповой задержки распространения сигнала  $\tau_g$  от центральной частоты его спектра  $f_p$  в рамках рассматриваемой модели частотной дисперсии описывается линейным законом. Оценивание наклона ДХ  $s$  происходит по методу наименьших квадратов по формуле:

$$\hat{s} = \sum_{j=1}^N \frac{\left( N f_{pj} - \sum_{i=1}^N f_{pi} \right) \hat{\tau}_j}{\left( N \sum_{i=1}^N f_{pi}^2 - \left( \sum_{i=1}^N f_{pi} \right)^2 \right)}, \quad (5)$$



где  $f_{pi}$  – центральная частота  $i$ -й подполосы;  $\hat{\tau}_j$  – измеренные задержки распространения сигналов в частотных подполосах посредством обработки их соответствующими согласованными фильтрами.

Оценка  $\hat{s}$  является линейной комбинацией независимых оценок  $\hat{\tau}_j$ , каждая из которых выполняется по критерию максимума правдоподобия. Тогда дисперсию оценки  $\hat{s}$  можно найти в форме:

$$\sigma_s^2 = \sum_{j=1}^N \left( \frac{Nf_{pj} - \sum_{i=1}^N f_{pi}}{N \sum_{i=1}^N f_{pi}^2 - \left( \sum_{i=1}^N f_{pi} \right)^2} \right)^2 \sigma_{\tau_j}^2, \quad (6)$$

где  $\sigma_{\tau_j}^2$  – дисперсия оценки задержки в сигнала в  $j$ -й подполосе. Дисперсию  $\sigma_{\tau_j}^2$  в предположении случайной начальной фазы можно вычислить по формуле:

$$\sigma_{\tau_j}^2 = \frac{1}{2E_j / N_0} \frac{1}{G_{2j}} \left[ 1 + \frac{1}{2E_j / N_0} \left[ 1 + \frac{G_{4j}}{G_{2j}^2} \right] \right], \quad (7)$$

где  $E_j$  – энергия сигнала в  $j$ -й подполосе,

$$F_{ij} = (N_s E_j)^{-1} \sum_{k=\lfloor (f_{pj}-0.5\Delta f/N)/F_s \rfloor}^{\lfloor (f_{pj}+0.5\Delta f/N)/F_s \rfloor} (2\pi f_k)^u |\dot{X}_k|^2;$$

$$E_j = \sum_{k=\lfloor (f_{pj}-0.5\Delta f/N)/F_s \rfloor}^{\lfloor (f_{pj}+0.5\Delta f/N)/F_s \rfloor} |\dot{X}_k|^2;$$

$$G_{2j} = F_{1j}^2 - E_j F_{2j}; \quad G_{4j} = 3F_{2j}^2 + E_j F_{4j} - 4F_{1j} F_{3j} - 3G_{2j}^2;$$

$F_s$  – частота дискретизации;  $\lceil x \rceil$  – округление в большую сторону;  $\lfloor x \rfloor$  – округление в меньшую сторону.

В отличие от дисперсии оценки наклона ДХ, полученной методом максимального правдоподобия, здесь  $\sigma_s^2$  зависит не только от формы спектра входного сигнала и ОСШ, но и от количества подполос  $N$ , на которые был разделен спектр сигнала.

В предположении использования широкополосных сигналов с равномерным спектром выражение (5) примет вид:

$$\sigma_{\text{МНК}S}^2 = \frac{3}{2\pi^2 \Delta f_n^2 (E/N_0)_n} \left[ 1 + \frac{7}{5} \frac{1}{(E/N_0)_n} \right] \sum_{j=1}^N \left( \frac{Nf_{pj} - \sum_{i=1}^N f_{pi}}{N \sum_{i=1}^N f_{pi}^2 - \left( \sum_{i=1}^N f_{pi} \right)^2} \right)^2, \quad (8)$$

где  $(E/N_0)_n = (E/N_0)/N$  – ОСШ в рамках одной подполосы сигнала. Здесь дисперсия оценки параметра  $s$  обратно пропорциональна второй степени ширины подполосы спектра сигнала  $\Delta f_n$ .

На рисунке 6 приведены расчетные кривые и отдельные выборочные значения СКО оценки  $s$ , полученные в

результате вычислительного эксперимента для предлагаемого метода и метода МП.

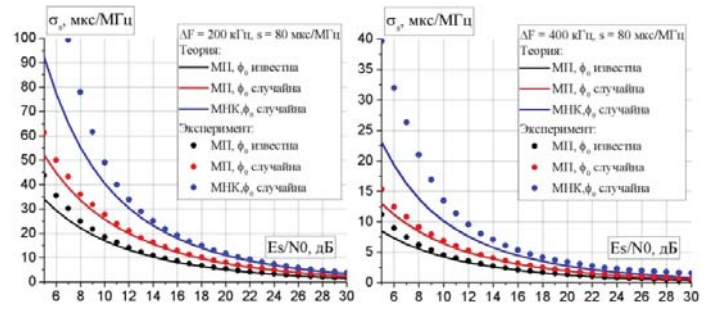


Рис. 6. СКО оценки  $s$  предлагаемым методом и методом МП

Как видно из рисунка 6, увеличение СКО оценки (ухудшение точности оценки) составляет около 2 раз по сравнению с методом МП при известной начальной фазе сигнала и примерно в 1,5 раза – при случайной начальной фазе.

Несмотря на то, что предлагаемый алгоритм, разумеется, проигрывает методу МП в точности оценки наклона ДХ ионосферного канала, его техническая реализация проще. Действительно, для оценки задержки технически проще реализовать на подполосы сигнала отдельные согласованные фильтры, чем набор фильтров, согласованных с сигналом, и учитывая при этом различные предполагаемые варианты значений  $s$  из области оценки. Согласованных фильтров требуется меньше.

### Исследование влияния оценки наклона дисперсионной характеристики при совместной оценке нескольких параметров широкополосных сигналов

Комплексная огибающая сигнала на выходе квадратурного демодулятора представлена в виде смеси комплексной огибающей полезного сигнала, искаженного частотной дисперсией ионосферного канала, и комплексной огибающей белого гауссовского шума

$$\hat{x}(t, \varphi, \tau, f_d, s) = e^{-j\varphi} e^{j2\pi f_d(t-\tau)} \hat{x}(t-\tau, s) + \dot{n}(t), \quad (9)$$

$$t = -T_s / 2 \div T_s / 2$$

где  $\hat{x}(t, s) = \hat{x}(t) * \hat{h}(t, s)$  – комплексная огибающая полезного сигнала, искажённой ионосферным каналом,  $\hat{h}(t, s)$  – комплексная огибающая импульсной характеристики (ИХ) ионосферного канала,  $\hat{x}(t)$  – комплексная огибающая полезного неискажённого сигнала,  $f_d$  – доплеровский сдвиг частоты,  $\tau$  – задержка,  $s$  – наклон дисперсионной характеристики – параметр, характеризующий дисперсионные искажения,  $\varphi$  – неизвестный фазовый сдвиг,  $\dot{n}(t)$  – комплексная огибающая белого гауссовского шума с нулевым средним и дисперсией;  $\sigma_{\text{ш}}^2$ ,  $T_s$  – длительность сигнала.

При когерентном оценивании решение о близости того или иного значения оценки к истинному значению определяемого параметра принимается по максимуму вещественной части корреляционного интеграла [64]:

$$\lambda = \max \left( \operatorname{Re} \left[ \int_{-T_s/2}^{T_s/2} \dot{y}(t) \tilde{u}^*(t, \hat{f}_d, \hat{\tau}, \hat{s}, \hat{\varphi}) dt \right] \right), \quad (10)$$

$\dot{y}(t)$  – аддитивная смесь квадратур полезного сигнала и белого гауссовского шума в непрерывном времени, определяемая по (9),  $\tilde{u}(t, \hat{f}_d, \hat{\tau}, \hat{s}, \hat{\varphi})$  – опорный сигнал, сформированный на основе априорных сведений о полезном сигнале,  $\hat{f}_d$  – оценка доплеровского сдвига,  $\hat{\tau}$  – оценка задержки,  $\hat{s}$  – оценка наклона ДХ,  $\hat{\varphi}$  – оценка начальной фазы, \* – символ комплексного сопряжения.

Корреляционный интеграл (10) можно представить в виде совокупности сигнальной и шумовой составляющей следующим образом:

$$\operatorname{Re} \left[ \int_{-T_s/2}^{T_s/2} \dot{y}(t) \tilde{u}^*(t, f_d, \tau, s, \varphi) dt \right] = S(f_d, \hat{f}_d, \tau, \hat{\tau}, s, \hat{s}, \varphi, \hat{\varphi}) + N(\hat{f}_d, \hat{\tau}, \hat{s}, \hat{\varphi}),$$

где  $S(f_d, \hat{f}_d, \tau, \hat{\tau}, s, \hat{s}, \varphi, \hat{\varphi})$  – вещественная часть сигнальной составляющей корреляционной суммы,  $N(\hat{f}_d, \hat{\tau}, \hat{s}, \hat{\varphi})$  – вещественная часть шумовой составляющей корреляционной суммы. Запишем аналитическое выражение для  $S(f_d, \hat{f}_d, \tau, \hat{\tau}, s, \hat{s}, \varphi, \hat{\varphi})$ :

$$S(f_d, \hat{f}_d, \tau, \hat{\tau}, s, \hat{s}, \varphi, \hat{\varphi}) = \operatorname{Re} \left[ e^{-j(\varphi_0 - \hat{\varphi}_0)} e^{-j2\pi f_d \tau} e^{j2\pi \hat{f}_d \hat{\tau}} \frac{1}{E_s} \int_{-\infty}^{\infty} \dot{x}(t - \tau, s) \dot{x}^*(t - \hat{\tau}, \hat{s}) e^{j2\pi(f_d - \hat{f}_d)t} dt \right] \quad (11)$$

где  $\dot{x}(t - \tau, s)$  – задержанный и искажённый частотной дисперсией полезный сигнал  $\dot{x}(t)$ ,  $\dot{x}(t - \hat{\tau}, \hat{s})$  – опорный сигнал,  $E_s$  – энергия сигнала  $\dot{x}(t)$ .

Для анализа качества совместной оценки  $f_d, \tau, s, \varphi$  необходимо вычислить дисперсии оценок всех исследуемых параметров и их взаимную корреляцию.

Корреляция оценки неизвестных параметров в первом приближении равна [64]

$$K_{ik}(\mathbf{I}_m, \mathbf{I}) = \frac{A_{ki}}{\rho^2 \Omega} \Big|_{\mathbf{I}_m \rightarrow \mathbf{I}}, \quad (12)$$

где  $\Omega$  – определитель матрицы  $W$ , состоящей из набора частных производных  $-\frac{\partial^2 S}{\partial l_i \partial l_j}$ ,  $S$  – вещественная часть сигнальной составляющей корреляционного интеграла (компактная запись),  $A_{ki}$  – алгебраические дополнения матрицы  $W$ ,  $\mathbf{I}_m$  – вектор оценок,  $\mathbf{I}$  – вектор оцениваемых параметров,  $i = 1 \div K, k = 1 \div K, K$  – количество оцениваемых параметров (в рассматриваемом в статье случае  $K = 4$ ),  $\rho^2 = 2E_s / N_0$  – отношение сигнал-шум (ОСШ),  $N_0$  – спектральная плотность мощности (СПМ) белого гауссовского

шума. Для совпадающих индексов  $i$  и  $k$  (12) соответствует дисперсиям оценок исследуемых параметров.

Выражение для коэффициента корреляции можно записать как

$$r_{ik}(\mathbf{I}_m, \mathbf{I}) = \frac{K_{ik}(\mathbf{I}_m, \mathbf{I})}{\sqrt{K_{ii}(\mathbf{I}_m, \mathbf{I})K_{kk}(\mathbf{I}_m, \mathbf{I})}}, \quad i = 1 \div K, \quad k = 1 \div K, \quad i \neq k.$$

Составим матрицу  $W$  для четырёх оцениваемых параметров:  $f_d, \tau, s, \varphi$ . Так как все оцениваемые параметры являются неэнергетическими, то матрицу  $W$  можно представить как

$$W = - \begin{pmatrix} \frac{\partial^2 S}{\partial \hat{f}_d^2} & \frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{\tau}} & \frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{s}} & \frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{\varphi}} \\ \frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{\tau}} & \frac{\partial^2 S}{\partial \hat{\tau}^2} & \frac{\partial^2 S}{\partial \hat{\tau} \partial \hat{s}} & \frac{\partial^2 S}{\partial \hat{\tau} \partial \hat{\varphi}} \\ \frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{s}} & \frac{\partial^2 S}{\partial \hat{\tau} \partial \hat{s}} & \frac{\partial^2 S}{\partial \hat{s}^2} & \frac{\partial^2 S}{\partial \hat{s} \partial \hat{\varphi}} \\ \frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{\varphi}} & \frac{\partial^2 S}{\partial \hat{\tau} \partial \hat{\varphi}} & \frac{\partial^2 S}{\partial \hat{s} \partial \hat{\varphi}} & \frac{\partial^2 S}{\partial \hat{\varphi}^2} \end{pmatrix} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}}. \quad (13)$$

Проведя все необходимые математические преобразования и взяв пределы, получим следующие выражения для производных, составляющих матрицу (13):

$$\frac{\partial^2 S}{\partial \hat{f}_d^2} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -4\pi^2 \tau^2 + 8\pi^2 \tau \int_{-\infty}^{\infty} t |\dot{x}(t - \tau)|^2 dt - \frac{4\pi^2}{E_s} \int_{-\infty}^{\infty} t^2 |\dot{x}(t - \tau)|^2 dt,$$

$$\frac{\partial^2 S}{\partial \hat{\tau}^2} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -\frac{4\pi^2}{E_s} \int_{-\infty}^{\infty} f^2 |\dot{X}(j2\pi f)|^2 df - 4\pi^2 f_d^2,$$

$$\frac{\partial^2 S}{\partial \hat{s}^2} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -\frac{1}{E_s} \int_{-\infty}^{\infty} \pi^2 f^4 |\dot{X}(j2\pi f)|^2 df,$$

$$\frac{\partial^2 S}{\partial \hat{\varphi}^2} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -1,$$

$$\frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{\tau}} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = \operatorname{Re} \left( j2\pi \frac{1}{E_s} \int_{-\infty}^{\infty} (t - \tau) \dot{x}(t - \tau) \frac{\partial \dot{x}^*(t - \tau)}{\partial t} dt \right),$$

$$\frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{s}} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = \operatorname{Re} \left( j2\pi \frac{1}{E_s} \int_{-\infty}^{\infty} t \dot{x}(t, s) \frac{\partial \dot{x}^*(t, s)}{\partial s} dt \right),$$

$$\frac{\partial^2 S}{\partial \hat{f}_d \partial \hat{\varphi}} \Big|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = 0,$$



$$\left. \frac{\partial^2 S}{\partial \hat{\alpha} \partial \hat{s}} \right|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -2\pi^2 f \frac{1}{E_s} \int_{-\infty}^{\infty} f^2 |\dot{X}(j2\pi f)|^2 df - \frac{1}{E_s} 2\pi^2 \int_{-\infty}^{\infty} f^3 |\dot{X}(j2\pi f)|^2 df,$$

$$\left. \frac{\partial^2 S}{\partial \hat{\omega} \partial \hat{\varphi}} \right|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -2\pi f_d,$$

$$\left. \frac{\partial^2 S}{\partial \hat{s} \partial \hat{\varphi}} \right|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}} = -\pi \frac{1}{E_s} \int_{-\infty}^{\infty} f^2 |\dot{X}(j2\pi f)|^2 df,$$

где  $\frac{\partial \dot{x}^*(t, s)}{\partial s} = j\pi \int_{-\infty}^{\infty} f^2 \dot{X}^*(-j2\pi f) H(-j2\pi f) e^{j2\pi f t} df$ ,  $\dot{X}(j2\pi f)$  –

комплексный спектр сигнала  $\dot{x}(t)$ . Заметим, что в производ-

ной  $\left. \frac{\partial^2 S}{\partial \hat{\alpha} \partial \hat{s}} \right|_{\substack{\hat{f}_d \rightarrow f_d \\ \hat{\tau} \rightarrow \tau \\ \hat{s} \rightarrow s \\ \hat{\varphi} \rightarrow \varphi}}$  интеграл  $\frac{1}{E_s} 2\pi^2 \int_{-\infty}^{\infty} f^3 |\dot{X}(j2\pi f)|^2 df = 0$ , если

спектр сигнала симметричен относительно  $f = 0$ .

Подставив полученные производные в (13), вычислив  $\Omega$  и алгебраические дополнения  $A_{ki}$ ,  $i=1 \div K$ ,  $k=1 \div K$ ,  $K=4$  матрицы  $W$ , можно определить все необходимые корреляционные связи между оценками неизвестных параметров с помощью выражения (12).

На рисунках 7-10 приведены графики зависимости СКО наклона ДХ и коэффициентов корреляции между наклоном ДХ и другими оцениваемыми параметрами от ОСШ. На рисунках приведены как теоретические зависимости, так и полученные в ходе имитационного моделирования. Имитационное моделирование было проведено с использованием одиночного прямоугольного импульса с шириной спектра 400 кГц. Наклон ДХ  $s$  был задан 60 мкс/МГц, частотный сдвиг  $f_d - 5$  Гц, задержка  $\tau - 0.1$  мкс, фазовый сдвиг  $\varphi - 90$  градусов. В результате моделирования были получены значения  $\hat{s}$ ,  $\hat{f}_d$ ,  $\hat{\tau}$  и  $\hat{\varphi}$ , была вычислена выборочная дисперсия и взаимная корреляция оценок для различных значений ОСШ. Количество экспериментов составило 1000. Из приведённых зависимостей можно сделать следующие выводы:

1. СКО оценки наклона ДХ при совместной его оценки с рядом параметров выше, чем при его одиночной оценке. Это связано с появлением взаимных корреляционных связей между оценками.

2. Корреляция между оценками наклона ДХ и задержки, наклона ДХ и частоты доплеровского сдвига отсутствует.

3. Присутствует корреляция между оценками  $\hat{s}$  и  $\hat{\varphi}$  показанная как теоретически, так и подтверждённая имитационным моделированием.

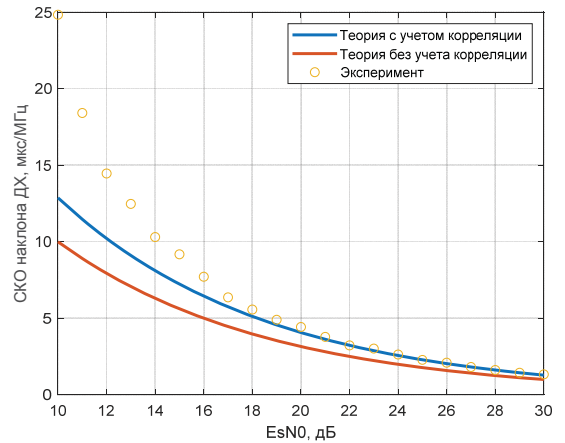


Рис. 7. СКО оценки наклона ДХ от ОСШ

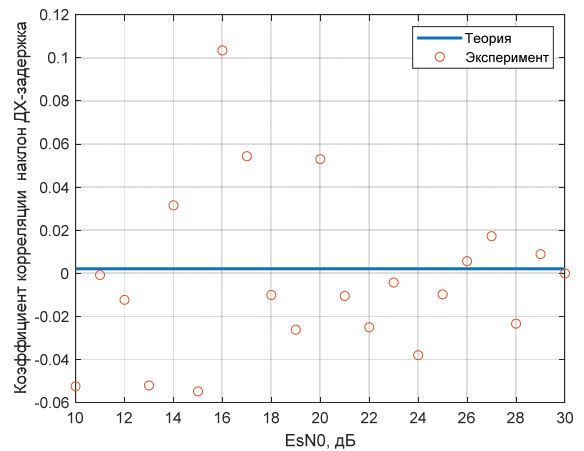


Рис. 8. Коэффициент корреляции между  $\tau$  и  $S$  в зависимости от ОСШ

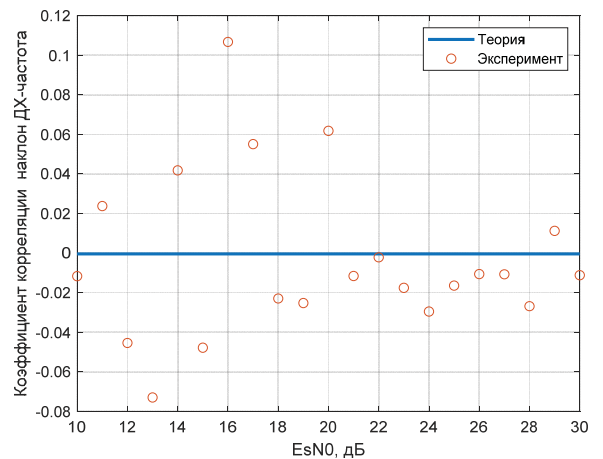


Рис. 9. Коэффициент корреляции между  $f_d$  и  $S$  в зависимости от ОСШ

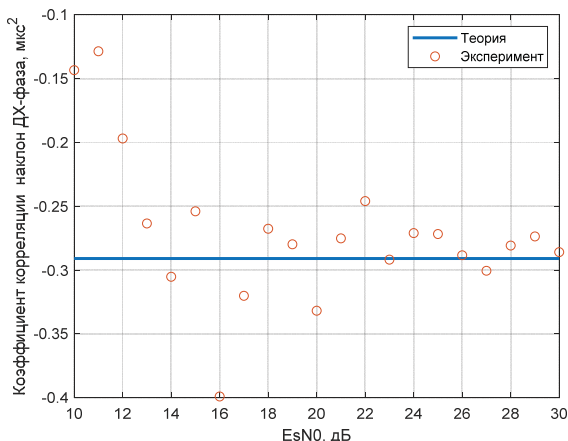


Рис. 10. Коэффициент корреляции между  $\varphi$  и  $S$  в зависимости от ОСШ

### Методы и алгоритмы компенсации дисперсионных искажений широкополосных сигналов

Компенсация во время обнаружения сигнала согласованным фильтром

Импульсная характеристика согласованного фильтра  $h_{сф}(t, s)$  примет вид:

$$h_{сф}(t, s) = u^*(T_0 - t, s), \quad (14)$$

где  $T_0$  – задержка, обусловленная физической реализуемостью СФ. Выражение для комплексной передаточной функции СФ  $H_{сф}(j\omega, s)$  имеет вид:

$$H_{сф}(j\omega, s) = e^{-j\omega T_0} X^*(j\omega) H^*(j\omega, s) = e^{-j\omega T_0} X^*(j\omega) e^{j\pi s \left(\frac{\omega}{2\pi}\right)^2}. \quad (15)$$

Более правильно в записи использовать не сам параметр  $s$ , а его оценку  $\hat{s}$ , полученную в результате зондирования или прогноза радиолинии:

$$\hat{H}_{сф}(j\omega, \hat{s}) = e^{-j\omega T_0} X^*(j\omega) H^*(j\omega, \hat{s}) = e^{-j\omega T_0} X^*(j\omega) e^{j\pi \hat{s} \left(\frac{\omega}{2\pi}\right)^2}. \quad (16)$$

На рисунке 11 представлена схема обнаружения сигнала с компенсацией дисперсионных искажений.

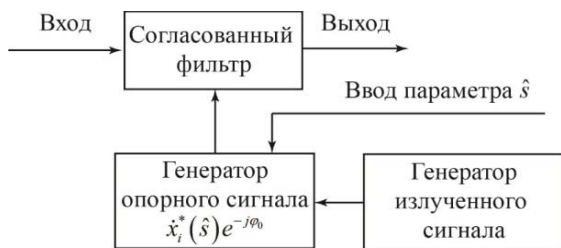


Рис. 11. Обнаружение сигнала с компенсацией дисперсионных искажений

### Компенсация с помощью банков цифровых фильтров

На рисунке 12 приведена схема банка фильтров с компенсацией частотной дисперсии [48, 49].

В приведенной схеме  $f_k$  – центральная частота  $k$ -го канала анализа-синтеза,  $n_k = n_{const} + \text{round}[sf_k f_0]$  – групповая задержка сигнала в  $k$ -ом канале анализа-синтеза, возникающая вследствие частотной дисперсии, выраженная в целом количестве отсчетов дискретизации  $T$ ,  $\text{round}(x)$  – функция округления до целого числа,  $n_{const}$  – некоторая константа, описывающая общую задержку сигнала,  $L - n_k$  – компенсационная задержка в  $k$ -ом канале.

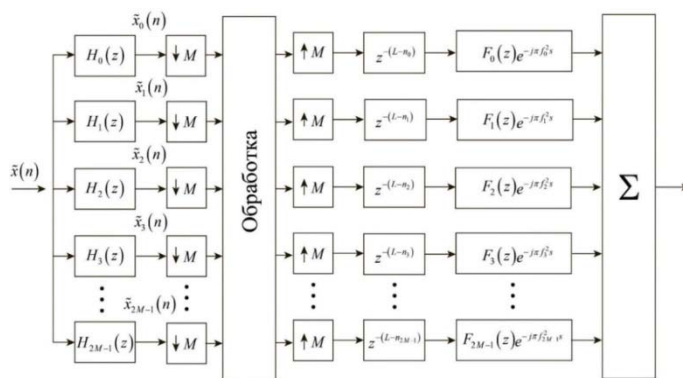


Рис. 12. Банк-фильтров с компенсацией частотной дисперсии

В результате компенсации, задержка сигнала во всех подканалах выравнивается до величины  $L$  отсчетов. Следует отметить, что компенсация групповой задержки происходит на высокой частоте дискретизации  $f_0$ , т.е. после процедуры интерполяции. Это позволяет скомпенсировать задержку с точностью до интервала дискретизации  $T = 1/f_0$ . Компенсационные линии задержки и фазовые множители (которые заранее учитываются в импульсных характеристиках фильтров синтеза) не требуют дополнительных вычислений.

На рисунке 13 приведена вычислительно упрощенная схема компенсации частотной дисперсии банком фильтров [55]. Для сокращения количества вычислительных операций, был применен алгоритм, изложенный в [60, 61]. Основная идея такого алгоритма состоит в представлении фильтров синтеза (и анализа) в виде набора полифазных компонент  $E_k(z)$  исходного фильтра прототипа, применении алгоритма БПФ Кули-Тьюки и обработке сигнала на низкой частоте дискретизации (т.е. до ее повышения в  $M$  раз).

Как видно из рисунка 13, схема компенсации частотной дисперсии, внедрённая в систему синтеза, претерпела изменения. В предлагаемой схеме компенсация групповой задержки осуществляется на низкой частоте дискретизации. При этом уже нельзя ограничиться внедрением компенсационных дискретных линий задержек, так как погрешность компенсации задержки будет в  $M$  раз больше (так как интервал дискретизации в  $M$  раз больше).



В таком случае возникает необходимость во внедрении интерполяционных фильтров, компенсирующих дробную задержку. Поэтому в схему компенсации внедрена система КИХ фильтров  $K_k(z)$ ,  $k = 0 \dots 2M - 1$ , устраняющих дробную задержку, посредством переоцифровки сигнала с помощью интерполяционного полинома порядка  $N_{poly} - 1$ , и линия задержки  $z^{-\tilde{n}_k}$ , устраняющая целую часть задержки,  $\tilde{n}_k = \tilde{n}_{const} + \text{round}(f_k s f_o M_0 / M)$ ,  $\text{round}(x)$  – функция, осуществляющее выделение целой части дробного числа  $x$ ,  $\tilde{n}_{const}$  – некоторая константа, описывающая общую задержку сигнала. Предварительная интерполяция в  $M_0$  раз осуществляется с целью уменьшения искажений сигнала, вызванных неравномерностью АЧХ и нелинейностью ФЧХ интерполяционного КИХ-фильтра.

Повышая предварительно частоту дискретизации в  $M_0$  раз, основной диапазон частот, в котором находится сигнал, расширяется. Это позволяет, обрабатывая одну копию сигнала в частотной области, уменьшить амплитудно-фазовые искажения, вносящие интерполяционным КИХ-фильтром при компенсации групповой задержки.

Значение  $M_0$  выбирается небольшим: 1 (без интерполяции), 2 или 4. Длина интерполяционного КИХ фильтра при этом равна  $N_{inter} = N_{poly} M_0 - 1$ .

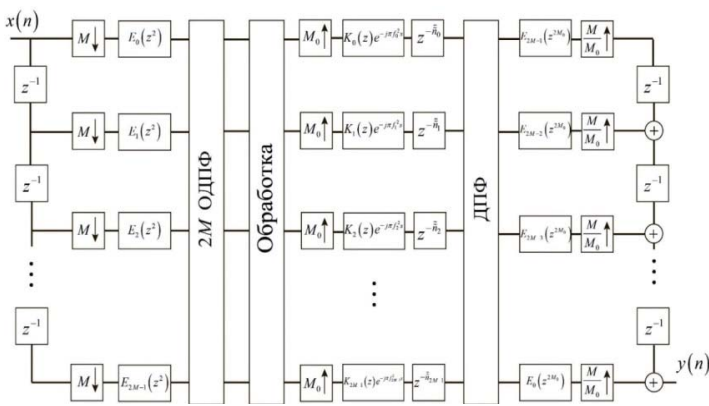


Рис. 13. Вычислительно упрощенная схема банка фильтров с компенсацией частотной дисперсии

На рисунке 14 приведены отклики СФ на широкополосный сигнал с учетом и без корректировки дисперсионных искажений с помощью банков фильтров. Уровень пика ВКФ при этом вырос на 6 дБ.

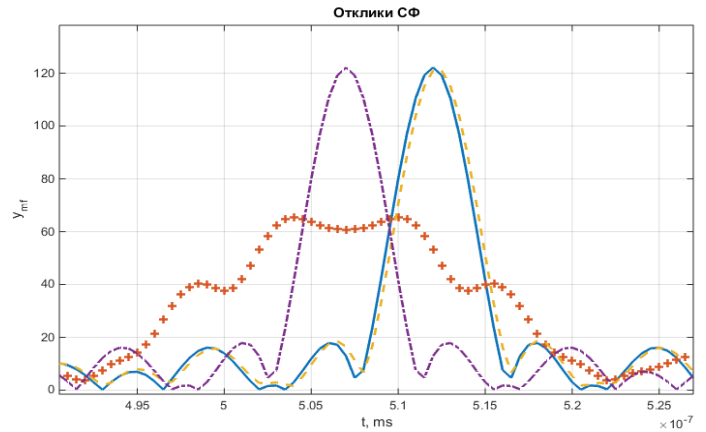


Рис. 14. Огибающие откликов согласованного фильтра на сигнал, предварительно обработанный банком фильтров (“-” – отклик СФ на неискажённый ионосферой сигнал, “+” – отклик СФ на искажённый ионосферой сигнал, “-.-” – отклик СФ на сигнал с компенсацией дисперсионных искажений, “-.-” – отклик СФ на сигнал с компенсацией дисперсионных искажений по выч. эф. алгоритму)

#### Обработка сигнала следящим компенсатором

Рассмотрим алгоритм следящей компенсации наклона ДХ. Запишем систему уравнений, состоящую из уравнения динамической системы и двух уравнений наблюдения (наблюдаем квадратуры на выходе квадратурного демодулятора):

$$\begin{cases} s_i = C_i s_{i-1} + \xi_i \\ y_{iRe} = u_{iRe}(s_i, \hat{s}_{oi}) + \eta_{iRe} \\ y_{iIm} = u_{iIm}(s_i, \hat{s}_{oi}) + \eta_{iIm} \end{cases}, \quad i = \overline{1 \div N}, \quad (17)$$

где  $\eta_{iRe}, \eta_{iIm}$  – белый гауссовский шум наблюдения,  $\xi_i$  – шум динамической системы,  $M[\eta_{iRe}] = M[\eta_{iIm}] = 0$  – математическое ожидание шумов  $\eta_{iRe}, \eta_{iIm}$ ,  $M[\xi_i] = 0$  – математическое ожидание шума  $\xi_i$ ,  $M[\dots]$  – операция вычисления математического ожидания,  $D[\eta_{iRe}] = D[\eta_{iIm}] = \sigma_\eta^2$  – дисперсия шумов  $\eta_{iRe}, \eta_{iIm}$ ,  $D[\xi_i] = \sigma_\xi^2$  – дисперсия шума,  $\xi_i$ ,  $D[\dots]$  – операция вычисления дисперсии,  $N$  – длина выборки,  $\hat{s}_{oi}$  – оптимальная оценка наклона ДХ  $s$ ,

$$\begin{aligned} u_i(s_i) &= \sum_{k=-N/2}^{N/2-1} \hat{X}_k \hat{X}_k^* e^{-j\pi f_k^2 (s_i - \hat{s}_{oi})}; u_{iRe}(s_i) = \\ &= \text{Re}(u_i(s_i)); u_{iIm}(s_i) = \text{Im}(u_i(s_i)) \end{aligned} \quad (18)$$

– нелинейные относительно оцениваемого параметра  $s$  функции уравнений наблюдения, учитывающие оценку наклона ДХ  $\hat{s}_{oi}, \hat{X}_k$  – спектральные отсчёты полезного сигнала,  $\hat{X}_k^*$  – комплексно-сопряженные отсчеты оценки сигнала, при приеме преамбулы  $\hat{X}_k^* = \hat{X}_k^*$ ,  $s_i$  – отсчеты оцениваемого случайного процесса, – наклона ДХ  $s$ .

Наклон ДХ  $s$  будем считать медленно изменяющимся случайным образом параметром. Проведём линеаризацию уравнений наблюдения разложением нелинейных функций  $u_{iRe}(s_i)$ ,  $u_{iIm}(s_i)$  в ряд Тейлора до линейного члена в окрестностях точки  $C_i \hat{s}_{i-1}$  и подставим полученный результат в уравнения наблюдения системы уравнений

$$\begin{cases} s_i = C_i s_{i-1} + \xi_i \\ y_{iRe} = a_1 s_i + b_1 + \eta_{iRe} \\ y_{iIm} = a_2 s_i + b_2 + \eta_{iIm} \end{cases}, \quad i = \overline{1 \div N}, \quad (19)$$

где

$$a_1 = u'_{iRe}[C_i \hat{s}_{i-1}], \quad b_1 = u_{iRe}[C_i \hat{s}_{i-1}] - u'_{iRe}[C_i \hat{s}_{i-1}] C_i \hat{s}_{i-1},$$

$$a_2 = u'_{iIm}[C_i \hat{s}_{i-1}], \quad b_2 = u_{iIm}[C_i \hat{s}_{i-1}] - u'_{iIm}[C_i \hat{s}_{i-1}] C_i \hat{s}_{i-1},$$

$$u'_{iRe}[C_i \hat{s}_{i-1}] = \sum_{k=-N/2}^{N/2-1} -j\pi f_k^2 \dot{X}_k \hat{X}_k^* e^{-j\pi f_k^2 (C_i \hat{s}_{i-1} - \hat{s}_{oi})},$$

$$u'_{iRe}[C_i \hat{s}_{i-1}] = \text{Re} \left( \sum_{k=-N/2}^{N/2-1} -j\pi f_k^2 \dot{X}_k \hat{X}_k^* e^{-j\pi f_k^2 (C_i \hat{s}_{i-1} - \hat{s}_{oi})} \right)$$

$$u'_{iIm}[C_i \hat{s}_{i-1}] = \text{Im} \left( \sum_{k=-N/2}^{N/2-1} -j\pi f_k^2 \dot{X}_k \hat{X}_k^* e^{-j\pi f_k^2 (C_i \hat{s}_{i-1} - \hat{s}_{oi})} \right).$$

Ниже приведён прямой алгоритм нелинейной фильтрации наклона ДХ с учётом выражения (19)

$$\hat{s}_i = C_i \hat{s}_{i-1} + \mathbf{K}_i [\mathbf{Y}_i - \mathbf{F}_i], \quad i = \overline{1 \div N}, \quad (20)$$

$$\mathbf{K}_i = \mathbf{A}_i \mathbf{P}_i [\mathbf{A}_i \mathbf{P}_i \mathbf{A}_i^T + \mathbf{Q}]^{-1}, \quad i = \overline{1 \div N}, \quad (21)$$

$$\mathbf{P}_i = C_i^2 \Gamma_{i-1} + B, \quad i = \overline{1 \div N}, \quad (22)$$

$$\Gamma_i = \mathbf{P}_i - \mathbf{K}_i \mathbf{A}_i \mathbf{P}_i, \quad i = \overline{1 \div N}, \quad (23)$$

где  $\mathbf{Y}_i = \begin{bmatrix} y_{iRe} \\ y_{iIm} \end{bmatrix}$  – вектор уравнений наблюдения,

$$\mathbf{F}_i = \begin{bmatrix} u_{iRe}[C_i \hat{s}_{i-1}] \\ u_{iIm}[C_i \hat{s}_{i-1}] \end{bmatrix}, \quad \mathbf{A}_i = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \quad \mathbf{\Gamma}_0 = \sigma_\eta^2 \mathbf{I}_{2 \times 2},$$

$\mathbf{Q} = M[\eta_i \eta_i^T]$ ,  $B = \sigma_\xi^2$ ,  $\mathbf{I}_{1 \times 1}$  – единичная матрица размера  $1 \times 1$ ,  $\hat{s}_0$  выбирается из априорных сведений. Оценка  $\hat{s}_{oi} = C_i \hat{s}_{i-1}$ ,  $i = \overline{1 \div N}$ ,  $\hat{s}_{o1} = C_1 \hat{s}_0$ . Это значит, что после каждой итерации каждому новому отсчёту управляющего воздействия  $\hat{s}_{oi}$  переписывается только рассчитанное значение  $C_i \hat{s}_{i-1}$ .

На рисунке 15 приведены кривые изменения наклона  $s$ , истинная и оцененная при  $E_s / N_0 = 7$  дБ.

Предполагается, что начальное значение наклона известно исходя из оценки по МП на этапе обнаружения сигнала и равно  $s_0 = 70 \text{ мкс} / \text{МГц}$ .

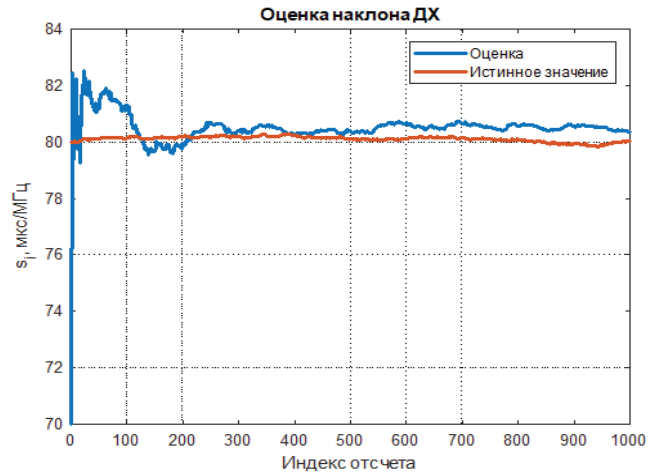


Рис. 15. Кривые изменения наклона  $s$

Алгоритм приема сигнала с оценкой и корректировкой дисперсионных искажений

На рисунке 16 приведена схема приема широкополосного сигнала с компенсацией дисперсионных искажений.

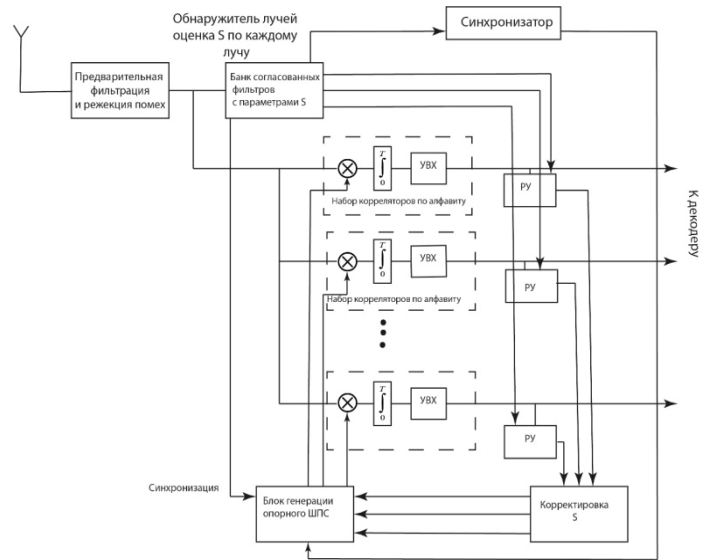


Рис. 16. Схема приема широкополосного сигнала с компенсацией дисперсионных искажений

После приемника квадратурные цифровые отсчеты с выхода демодулятора поступают на вход модуля предварительной фильтрации. Затем оцифрованные отсчеты подаются на обнаружитель лучей [62], содержащий согласованные фильтры с начальными значениями наклона дисперсионной характеристики  $s$ . Также оцифрованные отсчеты идут на множитель с опорными ШПС, после чего подаются на решающее устройство (РУ) для блока корректировки наклона дисперсионной характеристики  $s$  и к декодеру. Разработанный и описанный выше алгоритм положен в основу программной модели устройства обнаружения и приема сигнала с компенсацией дисперсионных искажений [64].

### Результаты натуральных экспериментов

В данном разделе приведены результаты эксперимента по компенсации дисперсионных искажений у широкополосного сигнала на однокачковой трассе протяженностью ~2900 км. В эксперименте использовался широкополосный сигнал с прямым расширением спектра псевдослучайной последовательностью, состоящей из 512 символов, ширина главного лепестка спектра сигнала составляла 400 кГц.

Среди экспериментальных записей сигналов были отобраны те, где присутствует минимальное количество стационарных помех. Рабочие частоты выбирались вблизи МПЧ, 0.85-1.05 от прогнозируемой, т.к. на них дисперсионные искажения значительны. Компенсация проводилась предложенными в статье методами, основанными на банках фильтров анализа-синтеза. Наклон ДХ был предварительно оценён по методу максимального правдоподобия.

В ходе проведения эксперимента было обработано пять различных записей, построены отклики СФ для необработанного банком фильтров сигнала, сигнала с компенсацией, внедрённой в классическую схему банка фильтров, и сигнала с компенсацией, внедрённой в вычислительно эффективную схему банка фильтров (см. рис. 17-20), а также определен выигрыш при компенсации.

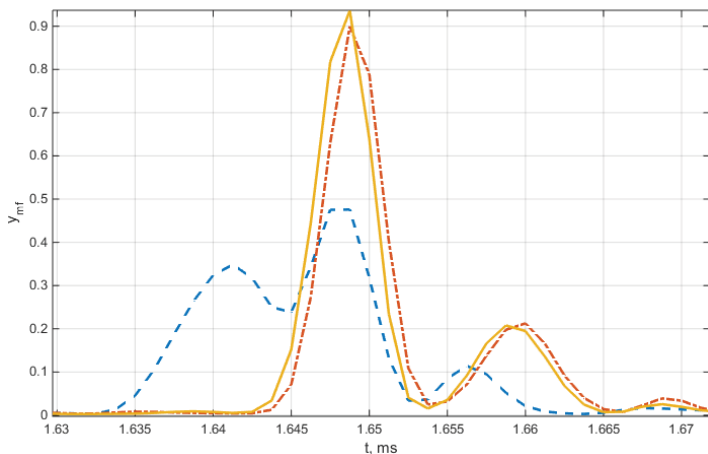


Рис. 17. Экспериментально полученные отклики СФ при  $s = 80$  мкс/МГц (запись 1)

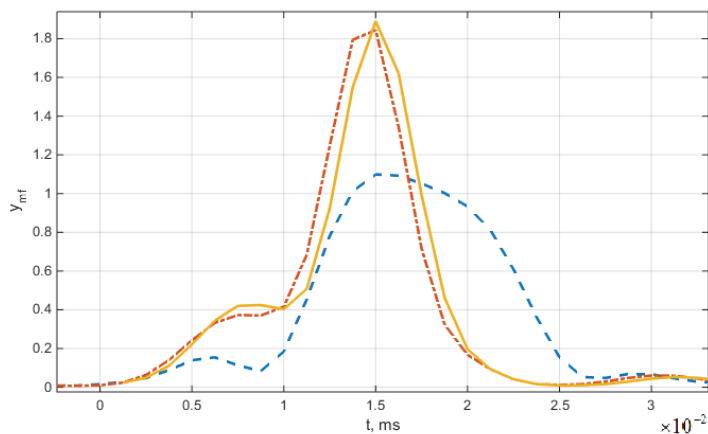


Рис. 18. Экспериментально полученные отклики СФ при  $s = 80$  мкс/МГц (запись 2)

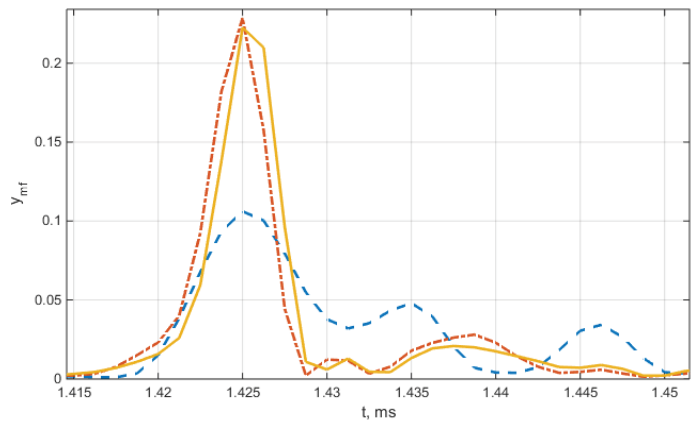


Рис. 19. Экспериментально полученные отклики СФ при  $s = 80$  мкс/МГц (запись 3)

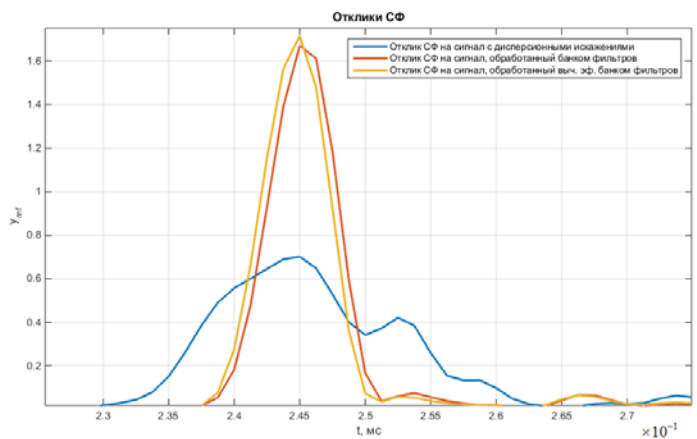


Рис. 20. Экспериментально полученные отклики СФ при  $s = 140$  мкс/МГц (запись 3)

Графики на рисунках 21-23 показывают влияние величины рассогласования истинного значения наклона ДХ и его оценки на ОСШ и фазовый сдвиг сигнала на выходе СФ. Фазовый сдвиг при отсутствии рассогласования обусловлен истинным значением начальной фазы сигнала.

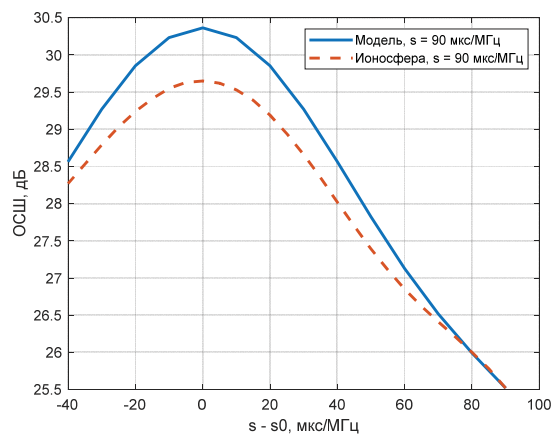


Рис. 21. Зависимость ОСШ на выходе СФ от величины рассогласования

Таблица 1

Качество компенсации

Номер записи исследуемого сигнала	Наклон ДХ $S$ , мкс/МГц	Теоретически ожидаемый выигрыш, дБ	$K_{кл.комп}$ , дБ	$K_{эф.комп}$ , дБ	$\Delta K$ , дБ
1	8	4.4	2.8	2.9	0.1
2	8	4.4	2.2	2.4	0.2
3	8	4.4	3.3	3.3	0.1
4	14	6.7	3.8	3.9	0.1

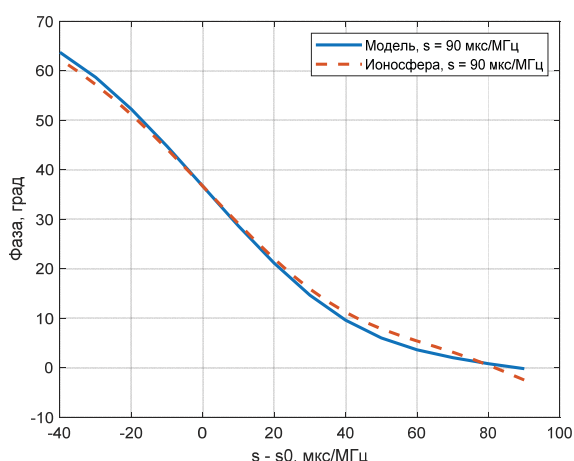


Рис. 22. Зависимость фазового сдвига от величины рассогласования

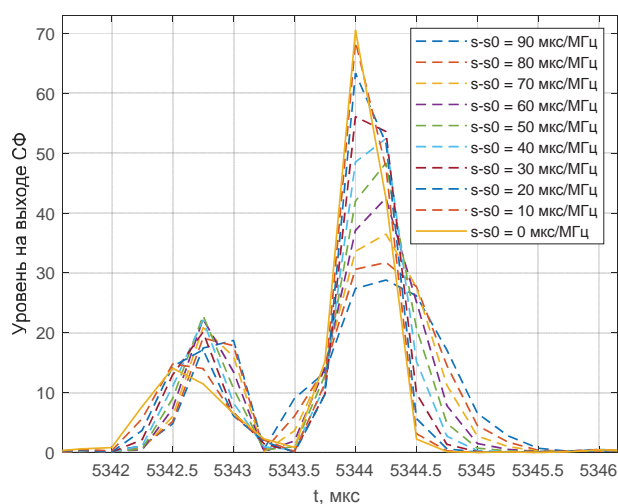


Рис. 23. Форма откликов СФ при различном компенсируемом значении наклона дисперсионной характеристики  $s$

Выигрыш при компенсации определяется как

$$K_{кл.комп} = 20 \lg \left[ \frac{\max(|\dot{q}_{комп}(n_*)|)}{\max(|\dot{q}(n_*)|)} \right] \text{ и}$$

$$K_{эф.комп} = 20 \lg \left[ \frac{\max(|\dot{q}_{эф.комп}(n_*)|)}{\max(|\dot{q}(n_*)|)} \right]$$

для классической и вычислительно эффективной схемы банка фильтров соответственно. Разница между выигрышем при двух видах компенсации равна  $\Delta K = |K_{эф.комп} - K_{кл.комп}|$ . Результаты эксперимента сведены в таблицу 1.

Из приведённых в таблице 1 значений видно, что при внедрении алгоритма компенсации частотной дисперсии выигрыш существенен (максимальный 3.9 дБ и минимальный 1.6 дБ для различных записей). Как и при теоретических расчётах, выигрыш при компенсации банком фильтров по вычислительно эффективному алгоритму немного больше, чем выигрыш при использовании классической схемы банка фильтров. Разница в выигрыше между этими двумя алгоритмами составила около 0.1 дБ.

### Заключение

Данная статья посвящена аналитическому обзору полученных теоретических и экспериментальных результатов оценки и компенсации дисперсионных искажений широкополосных сигналов, полученных коллективом МТУСИ.

В статье рассмотрены методы оценки наклона дисперсионной характеристики, а именно, оценка методом максимального правдоподобия (МП), оценка методом деления сигнала на подполосы. У метода деления на подполосы СКО оценки (ухудшение точности оценки) больше примерно в 2 раза по сравнению с методом МП при известной начальной фазе сигнала и примерно в 1,5 раза – при случайной начальной фазе. Несмотря на то, что предлагаемый алгоритм, разумеется, проигрывает методу МП в точности оценки наклона ДХ ионосферного канала, его техническая реализация проще. Действительно, для оценки задержки технически проще реализовать на подполосы сигнала отдельные согласованные фильтры, чем набор фильтров, согласованных с сигналом, и учитывая при этом различные предполагаемые варианты значений  $s$  из области оценки. Согласованных фильтров потребуется меньше. Исследовано влияние оценки наклона дисперсионной характеристики на качество оценивания других параметров радиосигнала. Показано, что существует корреляция между оценками наклона дисперсионной характеристики и фазового сдвига сигнала. Рассчитан коэффициент корреляции между ними.

Предложены методы и алгоритмы компенсации дисперсионных искажений широкополосных сигналов. Первый метод: компенсация во время обнаружения сигнала согласованным фильтром. Второй метод: компенсация с помощью банков цифровых фильтров. Третий метод: обработка сигнала следящим компенсатором.



Приведены результаты натурных экспериментов по компенсации дисперсионных искажений у широкополосного сигнала на одноканальной трассе протяженностью около 2900 км. Среди экспериментальных записей сигналов были отобраны те, где присутствует минимальное количество стационарных помех. Рабочие частоты выбирались вблизи МПЧ, 0.85-1.05 от прогнозируемой, так как на них дисперсионные искажения значительны.

В ходе проведения эксперимента было обработано пять различных записей, построены отклики СФ для необработанного банком фильтров сигнала, сигнала с компенсацией, внедрённой в классическую схему банка фильтров, и сигнала с компенсацией, внедрённой в вычислительно эффективную схему банка фильтров, а также определен выигрыш при компенсации. При внедрении алгоритма компенсации частотной дисперсии выигрыш существенен (максимальный 3.9 дБ и минимальный 1.6 дБ для различных записей). Как и при теоретических расчётах, выигрыш при компенсации банком фильтров по вычислительно эффективному алгоритму немного больше, чем выигрыш при использовании классической схемы банка фильтров. Разница в выигрыше между этими двумя алгоритмами составила около 0.1 дБ.

## Литература

1. MIL-STD-188-110C. Department of Defence interface standard. Interoperability and performance standards for data modems. US Department of Defense. 3 January 2012.
2. Jorgenson M.B., Johnson R.W., Nelson R.W. An Extension of Wideband HF Capabilities // IEEE Military Communications Conference. 2013. P. 1202-1206.
3. Gong Y., Li Y. Greedy Adaptive Modulation Algorithm for Wideband HF Communications // 2019 IEEE 19th International Conference on Communication Technology (ICCT), 2019, pp. 1026-1031, doi: 10.1109/ICCT46805.2019.8947007.
4. Овчинников В.В. Цифровой SDR-эквайзер для работы быстрой ППРЧ диспергирующих ионосферных каналах широкополосной СВ связи // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. 2020. № 3 (47). С. 18-27.
5. Perry B.D. A New Wideband HF Technique for MHz-Bandwidth Spread-Spectrum Radio Communications // IEEE Communications Magazine. 1983. Vol. 21, № 6. P. 28-36.
6. Laraway S., Farhang-Boroujeny B. Performance Analysis of a Multicarrier Spread Spectrum System in Doubly Dispersive Channels With Emphasis on HF Communications // IEEE Open Journal of the Communications Society. 2020. PP(99) 10.1109/OJCOMS.2020.2986323.
7. Laraway S. A., Loera J., Moradi H., Farhang-Boroujeny B. Experimental results of FB-MC-SS on a wideband HF NVIS propagation channel // MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 711-716, doi: 10.1109/MILCOM.2016.7795412.
8. MIL-STD-188-110D. Department of Defence interface standard. Interoperability and performance standards for data modems. US Department of Defense. 29 December 2017.
9. Варламов О.В., Нгуен Д.К., Грычкин С.Е. Комбинирование синтетических методов высокоэффективного высокочастотного усиления // Т-Comm: Телекоммуникации и транспорт. 2021. Том 15. №9. С. 11-16.
10. Varlamov O. V. Power Capacity of HF Automatic Antenna Tuner Switched by PIN Diodes under Load Mismatch Conditions // 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Svetlogorsk, Russia, 2020, pp. 1-5, doi: 10.1109/SYNCHROINFO49631.2020.9166046.
11. Varlamov O.V., Gromorushkin V.N. High Efficiency Power Amplifier for IoT Applications: RF Path // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, pp. 1-5, 2020. (DOI: 10.1109/IEEECONF48371.2020.9078651)
12. Gromorushkin V.N., Varlamov O.V., Dolgopyatova A.V., Voronkov A.A. Operation Problems of the EER Transmitter with Narrowband Antenna // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, pp. 1-5, 2019. (DOI: 10.1109/SOSG.2019.8706736).
13. Varlamov O.V., Gromorushkin V.N. Class D Switching Power Amplifier with a Filter under Load Mismatch Conditions // 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), pp. 1-6, 2020. 10.1109/WECONF48837.2020.9131508)
14. Громорушкин В. Н. Особенности работы транзисторного КВ передатчика на резонансную антенну // Технологии информационного общества : Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20-21 марта 2019 года. М.: ООО "Издательский дом Медиа паблишер", 2019. С. 268-270.
15. Варламов О.В. Максимальная мощность коммутируемого р-и-п диодами антенно-согласующего устройства диапазона ВЧ при рассогласовании нагрузки // Т-Comm: Телекоммуникации и транспорт. 2020. Том 14. №10. С. 26-32.
16. Иванов Д.В. Методы и математические модели исследования распространения в ионосфере сложных декаметровых сигналов и коррекции их дисперсионных искажений – Йошкар-Ола: МарГТУ, 2006. 266 с.
17. Катков К.А., Пашищев В.П., Катков Е.К. Вероятность превышения пороговых величин флуктуаций электронной концентрации при ионосферных возмущениях // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №7. С. 19-28.
18. Бова Ю.И., Крюковский А.С., Лукин Д.С. Математическое моделирование распространения частотно-модулированных электромагнитных волн в ионосфере для задач радиосвязи // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №12. С. 22-32.
19. Лобов Е.М., Косилов И.С. Расчет помехоустойчивости широкополосных ионосферных радиолиний с применением шумоподобных сигналов на основе данных прогнозирования // Т-Comm: Телекоммуникации и транспорт. 2011. Т. 5. № 11. С. 68-70.
20. Кандауров Н.А. Сигнально-кодовые конструкции и алгоритм их обработки с автоматической компенсацией дисперсионных искажений для широкополосной декаметровой связи // Т-Comm: Телекоммуникации и транспорт. 2019. Том 13. №2. С. 76-79.
21. Даренский В.Д., Мишин М.Ю., Капусткин А.Ю. Большие системы дискретных частотных сигналов: правила построения и основные характеристики // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №5. С. 27-30
22. Даренский В. Д., Капусткин А. Ю., Головкин И. В. Помехоустойчивые сигнально-кодовые конструкции на основе больших систем дискретных частотных сигналов и турбоподобных кодов для КВ канала // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №9. С. 30-33
23. Никитин М. Л., Копысов А. Н., Хворенков В. В. и др. Методы синтеза составных частотно-временных сигналов // Вестник ИжГТУ имени М.Т. Калашникова. 2015. Т. 18. № 3(67). С. 93-97.
24. Романов Ю. В., Хмырова Н. П. Сравнение способов передачи сообщений сигналами систем МЧТ и ЧВС в режиме с быстрой ППРЧ // Техника радиосвязи. 2016. Вып. 3 (30). С. 7–22
25. Коробицын В. В., Романов Ю. В., Фролова Ю. В. Ускорение генерации ансамблей частотно-временных матриц за счет использования параллельных вычислений // Техника радиосвязи. 2016. Вып. 4 (31). С. 7-16.

26. Дворников С. В., Бальков А. А. Предложения по управлению скоростью передачи и помехоустойчивостью сигналов с перестановочной частотной модуляцией // Т-Comm: Телекоммуникации и транспорт. 2020. Том 14. №6. С. 20-26.
27. Голубев Е.А., Лобов Е.М., Кандауров Н.А., Шубин Д.Н. Новый класс двоичных псевдослучайных последовательностей с нелинейным алгоритмом формирования для систем связи с кодовым разделением абонентов // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №2. С. 76-80.
28. Лобов Е. М., Шубин Д. Н., Кандауров Н. А., Лобова Е. О. Новый класс многофазных псевдослучайных последовательностей с нелинейным алгоритмом формирования для защищенных радиолиний связи между беспилотными транспортными средствами и диспетчерскими центрами "умного города" // Т-Comm: Телекоммуникации и транспорт. 2020. Том 14. №8. С. 42-46.
29. Русанов В.Э. Ограничения уровня боковых лепестков автокорреляционной функции  $m$ -последовательностей при малых аргументах // Т-Comm: Телекоммуникации и транспорт. 2017. Том 11. №3. С. 62-65.
30. Lobov E. M., Varlamov V. O. Investigation of the Properties of an Filterbank Multicarrier Modem in a Broadband HF Channel // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, 2021, pp. 1-4, doi: 10.1109/SYNCHROINFO51390.2021.9488412.
31. Головкин И.В. Исследование сходимости итеративных алгоритмов обработки сигнально-кодовых конструкций с использованием дискретных частотных сигналов и турбо-подобных кодов // Т-Comm: Телекоммуникации и транспорт. 2016. Том 10. №3. С. 21-29.
32. Lobov E. M., Shubin D. N. A Narrow-Band Interference Compensation Device Based on a Digital Filter Bank for Broadband Low-Energy HF Radio Lines // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, 2019, pp. 1-6, doi: 10.1109/SOSG.2019.8706791
33. Дворников С.В., Марков Е.В., Маноши Э.А. Повышение помехозащищенности передач декаметровых радиоканалов в условиях непреднамеренных помех // Т-Comm: Телекоммуникации и транспорт. 2021. Том 15. №6. С. 4-9.
34. Русанов В.Э. Потери помехоустойчивости корреляционного приёма для сигнала с фазовыми флуктуациями в виде диффузионного процесса // Т-Comm: Телекоммуникации и транспорт. – 2016. Том 10. №3. С. 11-14.
35. Шолохов И.Д., Пустовойтов Е.Л. Исследование совместного влияния замираний полезного и мешающего сигналов в случае логнормального распределения на качество приема полезного сигнала // Т-Comm: Телекоммуникации и транспорт. 2016. Том 10. №6. С. 27-33.
36. Аджемов С.С., Ретинский В.Н. Селекция расщепленной ионосферной волны с помощью вращения поляризации приемной антенны // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №1. С. 4-8.
37. Аджемов С.С., Ретинский В.Н. Локация деполаризованной волны // Т-Comm: Телекоммуникации и транспорт. 2018. Том 12. №6. С. 4-8.
38. Букашкин С.А., Оглоблин А.В., Шишкин Д.С. Построение и алгоритм работы радиолинии по технологии ММО на основе адаптивных фазированных антенных решеток // Радиотехника. 2015. №4. С. 28-31.
39. Барабощин А.Ю., Бузов А.Л., Красильников А.Д. Перспективы реализации технологии ММО в ДКМВ диапазоне на основе использования передающих кольцевых антенных решеток // Радиотехника. 2012. № 6. С. 73-78.
40. Daniels R. C., Peters S. W. A New MIMO HF Data Link: Designing for High Data Rates and Backwards Compatibility // Proceedings of MILCOM 2013 - 2013 IEEE Military Communications Conference (pp. 1250–1255). November 18–20, San Diego, CA.
41. Kopysov A., Klimov I., Zagidullin Y., Muravev V., Muraveva O. The use of polarization characteristic of ionosphere for data communications // 2014 International Conference on Mechanical Engineering, Automation and Control Systems (MEACS), 2014, pp. 1-4, doi: 10.1109/MEACS.2014.6986926.
42. Оглоблин А.В. Предельно достижимые характеристики комплексов ДКМВ радиосвязи, реализующих технологию ММО, при различных видах разнесения // Электросвязь. 2015. №5. С. 47-51.
43. Лобов Е.М., Смердова Е.О. Оценка импульсной характеристики широкополосного ионосферного канала с помощью метода обратной фильтрации // Т-Comm: Телекоммуникации и транспорт. 2017. Том 11. №3. С. 24-27.
44. Лобов Е.М., Смердова Е.О. Исследование качества алгоритмов оценки наклона дисперсионной характеристики ионосферного канала // Электросвязь. 2017. № 6. С. 28-31.
45. Лобов Е.М., Смердова Е.О., Кандауров Н.А., Косилов И.С., Елсуков В.А. Optimum estimation and filtering of the ionospheric channel dispersion characteristics slope algorithms // Systems of signal synchronization, generating and processing in telecommunications (SINKHROINFO), 2017 (DOI: 10.1109/SINKHROINFO.2017.7997537)
46. Мирошникова Н.Е. Применение адаптивной фильтрации в задаче оценки ионосферного канала // Т-Comm: Телекоммуникации и транспорт. 2016. Том 10. №9. С. 24-29.
47. Лобов Е.М., Лобова Е.О., Кандауров Н.А. Оптимальный следающий компенсатор дисперсионных искажений широкополосных сигналов // Электросвязь. 2018. № 5. С. 85-89.
48. Лобов Е.М., Лобова Е.О., Елсуков В.А. Устройство компенсации дисперсионных искажений широкополосных сигналов на базе банка цифровых фильтров // Доклады 20-й международной конференции «Цифровая обработка сигналов и ее применение – DSPA-2018», Москва, Россия, Том 2., С.487-491
49. Lobova E.O., Lobov E.M., Elskov V.A. Wideband signals dispersion distortion compensator based on digital filter banks // 2018 Systems of signals generating and processing in the field of on board communications, Moscow, 14-15 March 2018, 4 p. DOI: 10.1109/SOSG.2018.8350615
50. Adjemov S. S., Lobov E. M., Kandaurov N. A. and Lobova E. O. Methods and algorithms of broadband HF signals dispersion distortion compensation // 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), 2019, pp. 1-9, doi: 10.1109/SYNCHROINFO.2019.8814074.
51. Lipatkin V. I., Lobov E. M., Lobova E. O., Kandaurov N. A., Cramer-Rao Bounds for Wideband Signal Parameters Joint Estimation in Ionospheric Frequency Dispersion Distortion Conditions, // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, 2021, pp. 1-7, doi: 10.1109/IEEECONF51389.2021.9416074.
52. Lipatkin V. I., Lobova E. O., Telengator K. E. The Influence of the Quality of the Estimation of Dispersion Distortions of a Broadband HF Signal on the Noise Immunity of a Radio Link // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, 2021, 1-5, d 10.1109/SYNCHROINFO51390.2021.9488371.
53. Лобов Е.М., Припутин В.С., Лобова Е.О., Либерман Е.А. Следающий компенсатор дисперсионных искажений на основе сигма-точечного фильтра Калмана // Т-Comm: Телекоммуникации и транспорт. 2021. Том 15. №1. С. 41-47.
54. Чиров Д.С., Лобова Е.О. Компенсатор дисперсионных искажений широкополосных сигналов декаметрового диапазона, построенный на базе банка цифровых фильтров. Теория и эксперимент // Т-Comm: Телекоммуникации и транспорт. 2020. Том 14. №4. С. 57-65.



55. Lobov E.M., Lobova E.O., Kurochkin A.A. Computationally simplified realization of the compensator of dispersion distortions on the basis of the filter bank // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, 4-5 July, 2018, 4 p. (DOI: 10.1109/SYNCHROINFO.2018.8457058)

56. Крейнделин В.Б., Григорьева Е.Д. Реализация банка цифровых фильтров с пониженной вычислительной сложностью // Т-Comm: Телекоммуникации и транспорт. 2019. Том 13. №7. С. 48-53.

57. Крейнделин В.Б., Григорьева Е.Д. Анализ быстрого алгоритма умножения матриц и векторов для банка цифровых фильтров // Т-Comm: Телекоммуникации и транспорт. 2021. Том 15. №1. С. 4-10.

58. Соколов К.Ю., Припутин В.С., Лобова Е.О. Реализация косинусно-модулированных цифровых фильтров на базе процессора с архитектурой ARM // Т-Comm: Телекоммуникации и транспорт. 2020. Том 14. №11. С. 57-63.

59. Shubin D. N., Lobov E. M., Lobova E. O., Kandaurov N. A. A Device for Processing a Wideband Signal of the HF Waveband Using a Digital Filter Bank // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, 2021, pp. 1-9, doi: 10.1109/SYNCHROINFO51390.2021.9488356.

60. Karp T., Fliege N.J. Modified DFT Filter Banks with Perfect Reconstruction // IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing, vol. 46, 11, P. 1404-1414, DOI: 10.1109/82.803480

61. Koilpillai R.D., Vaidyanathan P.P. Cosine-Modulated FIR Filter Banks Satisfying Perfect Reconstruction // IEEE Transactions on Signal Processing. Vol. 40. #4. 1992. P. 770-783.

62. Кандауров Н.А., Лобов Е.М. Оценка вероятностных характеристик алгоритма обнаружения серии шумоподобных сигналов в условиях широкополосного ионосферного канала // Системы синхронизации, формирования и обработки сигналов. 2016. Т. 7. № 1. С. 30-32.

63. Витязев В.В. Многоскоростная обработка сигналов. М.: Горячая линия – Телеком. 2017. 336 с.

64. Программный модуль обнаружения и приема широкополосных фазоманипулированных сигналов с автоматическим компенсатором дисперсионных искажений / Н.А. Кандауров [и др.] // Свидетельство о государственной регистрации программы для ЭВМ № 2018617993 от 05.07.2018.

65. Куликов Е.И., Трифонов А.П. Оценка параметров сигналов на фоне помех. М.: Сов. радио, 1978. 296 с.

## ALGORITHMS OF ESTIMATING AND COMPENSATING THE DISPERSION DISTORTIONS OF WIDEBAND SIGNALS IN THE HF CHANNEL

**SERGEY S. ADJEMOV**

Moscow, Russia

**EVGENIY M. LOBOV**

Moscow, Russia, lobov@srd.mtuci.ru

**NIKOLAI A. KANDAUROV**

Moscow, Russia, jet1992@yandex.ru

**ELIZAVETA O. LOBOVA**

Moscow, Russia, lizabeth2@mail.ru

**VLADISLAV I. LIPATKIN**

Moscow, Russia, lipatkin.24@gmail.com

**KEYWORDS:** *ionosphere, wideband telecommunication, dispersion distortion, signal parameter estimation, compensation*

### ABSTRACT

**Introduction:** radio communication in the decameter range is actively used for communication in remote and hard-to-reach regions of the world. Decameter communication is also a relevant type of radio communication for regions that have suffered serious damage due to natural disasters. The relevance of using decameter radio communication in the above cases is due to the fact that this technology can offer reliable and cheap solutions. The second area of application of decameter radio communications is communications in the Arctic and Antarctic. **Practical significance:** when receiving signals with a spread spectrum, it becomes necessary to take into account the effect of the frequency dispersion of the ionospheric channel, since it leads to significant distortions of the useful signal and a decrease in the quality of communication in general. An urgent task is to estimate the parameters

of the frequency dispersion of the ionospheric channel and to develop algorithms and devices for compensating dispersion distortions of broadband signals. **Discussion:** this article presents algorithms for estimating and compensating the dispersion distortions of wideband signals in the HF channel. The subbanding estimation method and maximum likelihood estimation (MLE) of the slope of the dispersion characteristic (the slope of DC) are studied. In addition, this article examines the joint MLE of the slope of DC and other parameters of the wideband signal and offers three methods of dispersion distortion compensation. The first method of compensation is a matched filter compensation. The second one is compensation based on the filter bank. Finally, the third method uses a tracking compensator to solve the problem. The experimental results demonstrated in the article were carried out on a one-jump track with a length of about 2900 km.



## REFERENCES

1. MIL-STD-188-110C. Department of Defence interface standard. Interoperability and performance standards for data modems. US Department of Defense. 3 January 2012.
2. M. B. Jorgenson, R. W. Johnson, R. W. Nelson (2013). An Extension of Wideband HF Capabilities. *IEEE Military Communications Conference*. Pp. 1202-1206.
3. Y. Gong, Y. Li (2019). Greedy Adaptive Modulation Algorithm for Wideband HF Communications. *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. Pp. 1026-1031, doi: 10.1109/ICCT46805.2019.8947007
4. V. V. Ovchinnikov (2020). Digital SDR-equalizer for operation of FHSS of dispersive ionospheric channels of broadband HF communication. *The messenger of Volga State University of Technology. Series: Radiotechnical and infocommunication systems*. No. 3 (47). Pp. 18-27.
5. B. D. Perry (1983). A New Wideband HF Technique for MHz-Bandwidth Spread-Spectrum Radio Communications. *IEEE Communications Magazine*. Vol. 21, No. 6. Pp. 28-36
6. S. Laraway, B. Farhang-Boroujeny (2020). Performance Analysis of a Multicarrier Spread Spectrum System in Doubly Dispersive Channels With Emphasis on HF Communications. *IEEE Open Journal of the Communications Society*. PP(99):1-1 DOI: 10.1109/OJCOMS.2020.2986323.
7. S. A. Laraway, J. Loera, H. Moradi, B. Farhang-Boroujeny (2016). Experimental results of FB-MC-SS on a wideband HF NVIS propagation channel. *MILCOM 2016 - 2016 IEEE Military Communications Conference*. Pp. 711-716, doi: 10.1109/MILCOM.2016.7795412.
8. MIL-STD-188-110D. Department of Defence interface standard. Interoperability and performance standards for data modems. US Department of Defense. 29 December 2017.
9. O. V. Varlamov, D.C. Nguyen, S. E. Grychkin (2021). Combination of synthetic high-performance RF amplification techniques. *T-Comm*, vol. 15, no.9. Pp. 11-16. (in Russian)
10. O. V. Varlamov (2020), "Power Capacity of HF Automatic Antenna Tuner Switched by PIN Diodes under Load Mismatch Conditions," 2020 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Svetlogorsk, **Russia**, 2020, pp. 1 FO49631.2020.9166046.
11. O. V. Varlamov and V. N. Gromorushkin (2020), "High Efficiency Power Amplifier for IoT Applications: RF Path", 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, pp. 1-5. (DOI: 10.1109/IEECONF48371.2020.9078651)
12. V. N. Gromorushkin, O. V. Varlamov, A. V. Dolgopyatova and A. A. Voronkov (2019), "Operation Problems of the EER Transmitter with Narrowband Antenna", 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, pp. 1-5. (DOI: 10.1109/SOSG.2019.8706736).
13. O. V. Varlamov and V. N. Gromorushkin (2020), "Class D Switching Power Amplifier with a Filter under Load Mismatch Conditions", 2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), pp. 1-6. (DOI: 10.1109/WECONF48837.2020.9131508)
14. V. N. Gromorushkin (2019). Particular qualities of the operation of a transistor HF transmitter to a resonant antenna. Technologies of the information society: Materials of the XIII International Industrial Scientific and Technical Conference, Moscow, 20-21 March 2019. Moscow: "Publishing House Media Publisher". Pp. 268-270.
15. O. V. Varlamov (2020). Maximum power of the HF antenna tuner switched by PIN diodes at load mismatch. *T-Comm*, vol. 14, no.10. Pp. 26-32. (in Russian)
16. D. V. Ivanov (2006). Methods and mathematical models for studying the propagation of complex HF signals in the ionosphere and correcting their dispersion distortions. Yoshkar-Ola: MarSTU, 2006. 266 p.
17. K. A. Katkov, V. P. Pashintsev, E. K. Katkov (2018). The probability of exceeding threshold values of fluctuations of the electron concentration at ionospheric disturbance. *T-Comm*, vol. 12, no.7. Pp. 19-28. (in Russian)
18. Yu. I. Bova, A. S. Kryukovsky, D. S. Lukin (2018). Mathematical modeling of propagation of frequency-modulated electromagnetic waves in the ionosphere for the problems of radiocommunication. *T-Comm*, vol. 12, no.12. Pp. 22-32. (in Russian)
19. E. M. Lobov, I. S. Kosilov (2011). Calculation of noise immunity of broadband ionospheric radio lines using noise-like signals based on prediction data. *T-Comm*, vol. 5, no.11. Pp. 68-70. (in Russian)
20. N. A. Kandaurov (2019). Signal-code constructs and processing algorithm with automatic dispersion distortion compensation for wideband HF communication. *T-Comm*, vol. 13, no.2. Pp. 76-79.
21. V. D. Darensky, M. Yu. Mishin, A. Yu. Kapustkin (2018). Big systems of discrete frequency signals: generation rules and basic characteristics. *T-Comm*, vol. 12, no.5. Pp. 27-30. (in Russian)
22. V. D. Darensky, A.Yu. Kapustkin, I. V. Golovkin (2018). Interference immunity signal-code structures generated on the big systems of discrete frequency signals and turbo-liked codes for HF-range channel. *T-Comm*, vol. 12, no.9. Pp. 30-33. (in Russian)
23. M. L. Nikitin, A. N. Kopisov, V. V. Hvorenkov and others (2015). Methods for the synthesis of composite time-frequency signals. *Messenger of Kalashnikov ISTU*. B. 18. No. 3(67). Pp. 93-97.
24. U. V. Romanov, N. P. Hmirova (2016). The comparison of methods for transmitting messages by signals of the MFSK and FTS systems in the mode with FHSS. *Technique of radio communication*. Release 3 (30). Pp. 7-22.
25. V. V. Korabnicin, U. V. Romanov, U. V. Frolova (2016). Acceleration of the generation of ensembles of time-frequency matrices due to the use of parallel computations. *Technique of radio communication*. Release 4 (31). Pp. 7-16.
26. S. V. Dvornikov, A. A. Balykov (2020). Proposals for management of the transmission speed and noise immunity of signals with permutation frequency modulation. *T-Comm*, vol. 14, no.6. Pp. 20-26.
27. E. A. Golubev, E. M. Lobov, N. A. Kandaurov, D. N. Shubin (2018). New class of binary pseudo-random sequences with a nonlin-



- ear generation algorithm for communication systems with CDMA. *T-Comm*, vol. 12, no.2. Pp. 76-80.
28. E. M. Lobov, D. N. Shubin, N. A. Kandaurov, E. O. Lobova (2020) A new class of polyphase pseudo-random sequences with a nonlinear generation algorithm for secure radio communication link between unmanned vehicles and dispatch centers of the "smart city". *T-Comm*, vol. 14, no.8. Pp. 42-46. (in Russian)
29. V. E. Rusanov (2017). Restriction of the m-sequence of side lobes for minor arguments. *T-Comm*, vol. 11, no.3. Pp. 62-65.
30. E. M. Lobov and V. O. Varlamov, "Investigation of the Properties of an Filterbank Multicarrier Modem in a Broadband HF Channel," *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO, 2021)*. Pp. 1-4, doi: 10.1109/SYNCHROINFO51390.2021.9488412.
31. I. V. Golovkin (2016). Investigation of convergence behavior of iterative algorithms in serial concatenation of discrete frequency signals and turbolike codes. *T-Comm*. Vol. 10. No.3. Pp. 21-29. (in Russian)
32. E. M. Lobov, D. N. Shubin (2019). A Narrow-Band Interference Compensation Device Based on a Digital Filter Bank for Broadband Low-Energy HF Radio Lines, *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*. Pp. 1-6, doi: 10.1109/SOSG.2019.8706791
33. S. V. Dvornikov, E.V. Markov, A. A. Manoshi (2021) Increasing immunity of decameter radio channel transmissions under unintended interference. *T-Comm*, vol. 15, no.6. Pp. 4-9. (in Russian)
34. V. E. Rusanov (2016). The loss of noise immunity for the correlational receiving of the signal with phase fluctuations represented as diffusion process. *T-Comm*. Vol. 10. No.3. Pp. 11-14. (in Russian)
35. I. D. Sholokhov, E. L. Pustovoitov (2016). The study of combined impact of fadings of useful and interfering signals in the case of log-normal distribution on the quality of the useful signal reception (part 1). *T-Comm*. 2016. Vol. 10. No.6. Pp. 27-33. (in Russian)
36. S. S. Adjemov, V. N. Repinsky (2018). Selection of the split ionospheric wave by means of rotation of polarization of the reception antenna. *T-Comm*, vol. 12, no.1. Pp. 4-8. (in Russian)
37. S. S. Adjemov, V. N. Repinsky (2018). Location of a depolarized wave. *T-Comm*, vol. 12, no.6. Pp. 4-8. (in Russian)
38. S. A. Bukashkin, A. V. Ogloblin, D. S. (2015). Shishkin Construction and operation algorithm of a radio link using MIMO technology based on adaptive phased antenna arrays. *Radiotechnic*. No. 4. Pp. 28-31.
39. A. U. Baraboshin, A. L. Buzov, A. D. Krasilnikov (2012). Prospects for the implementation of MIMO technology in the HF range based on the use of transmitting ring antenna arrays. *Radiotechnic*. No. 6. Pp. 73-78.
40. R. C. Daniels and S. W. Peters (2013). A New MIMO HF Data Link: Designing for High Data Rates and Backwards Compatibility. *Proceedings of MILCOM 2013 - 2013 IEEE Military Communications Conference*. Pp. 1250-1255. November 18-20, San Diego, CA.
41. A. Kopysov, I. Klimov, Y. Zagidullin, V. Muravev and O. Muraveva (2014). The use of polarization characteristic of ionosphere for data communications. *2014 International Conference on Mechanical Engineering, Automation and Control Systems (MEACS)*. Pp. 1-4, doi: 10.1109/MEACS.2014.6986926.
42. A. V. Ogloblin (2015). Maximum achievable characteristics of HF radio communication complexes implementing MIMO technology for various types of diversity. *Electrocommunications*. No.5. Pp. 47-51.
43. E. M. Lobov, E. O. Smerdova (2017). Broadband ionospheric channel impulse response estimation using the method of reverse filtering. *T-Comm*, vol. 11, no.3. Pp. 24-27. (in Russian)
44. E. M. Lobov, E. O. Smerdova (2017). The study of quality of estimation algorithms of the slope of dispersion characteristic of ionospheric channel. *Electrocommunications*. No. 6. Pp. 28-31.
45. E. M. Lobov, E. O. Smerdova, N. A. Kandaurov, I. S. Kosilov, B. A. Elsukov (2017). Optimum estimation and filtering of the ionospheric channel dispersion characteristics slope algorithms. *Systems of signal synchronization, generating and processing in telecommunications (SINKHROINFO)*, 2017. DOI: 10.1109/SINKHROINFO.2017.7997537
46. N. E. Miroshnikova (2016). Adaptive filtering for HF channel estimation. *T-Comm*. Vol. 10. No.9. Pp. 24-29. (in Russian)
47. E. M. Lobov, E. O. Lobova, N. A. Kandaurov (2018). The optimal tracking dispersion distortions compensator of wideband signals. *Electrocommunications*. No. 5. Pp. 85-89.
48. E. M. Lobov, E. O. Lobova, B. A. Elsukov (2018). The distortion compensation device for wideband signals based in the filter bank. *Reports of the 20th International Conference "Digital Signal Processing and its Application - DSPA-2018"*, Moscow, Russia, Book 2. Pp. 487-49
49. E. M. Lobov, E. O. Lobova, B. A. Elsukov (2018). Wideband signals dispersion distortion compensator based on digital filter banks. *2018 Systems of signals generating and processing in the field of on board communications*, Moscow, 14-15 March 2018, 4 p. DOI: 10.1109/SOSG.2018.8350615
50. S. S. Adjemov, E. M. Lobov, N. A. Kandaurov and E. O. Lobova (2019). Methods and algorithms of broadband HF signals dispersion distortion compensation. *2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*. Pp. 1-9, doi: 10.1109/SYNCHROINFO.2019.8814074.

51. V. I. Lipatkin, E. M. Lobov, E. O. Lobova and N. A. Kandaurov (2021). Cramer-Rao Bounds for Wideband Signal Parameters Joint Estimation in Ionospheric Frequency Dispersion Distortion Conditions. *2021 Systems of Signals Generating and Processing in the Field of on Board Communications*. Pp. 1-7, doi: 10.1109/IEECONF51389.2021.9416074.
52. V. I. Lipatkin, E. O. Lobova and K. E. Telengator (2021). The Influence of the Quality of the Estimation of Dispersion Distortions of a Broadband HF Signal on the Noise Immunity of a Radio Link. *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*. Pp. 1-5, doi: 10.1109/SYNCHROINFO51390.2021.9488371.
53. E. M. Lobov, V. S. Priputin, E. O. Lobova, E. A. Liberman (2021). Dispersion distortion tracking compensator based on the sigma-point Kalman. *T-Comm*, vol. 15, no.1. Pp. 41-47. (in Russian)
54. D. S. Chirov, E. O. Lobova (2020). Wideband HF signals dispersion distortion compensator based on digital filter banks. Theory and approbation. *T-Comm*, vol. 14, no.4. Pp. 57-65. (in Russian)
55. E. M. Lobov, E. O. Lobova, A. A. Kurochkin (2018). Computationally simplified realization of the compensator of dispersion distortions on the basis of the filter bank. *2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, Minsk, 4-5 July, 4 p. (DOI: 10.1109/SYNCHROINFO.2018.8457058)
56. V. B. Kreyndelin, E. D. Grigorieva (2019). The implementation of the bank of digital filters with reduced computational complexity. *T-Comm*, vol. 13, no.7. Pp. 48-53. (in Russian)
57. V. B. Kreyndelin, E. D. Grigorieva (2021) Analysis of fast algorithm of matrix-vector multiplication for the bank of digital filters. *T-Comm*, vol. 15, no.1. Pp. 4-10. (in Russian)
58. K. Yu. Sokolov, V. S. Priputin, E. O. Lobova (2020). Implementation of Cosine Modulated Digital Filter Bank on Processor with ARM architecture. *T-Comm*, vol. 14, no.11. Pp. 57-63. (in Russian)
59. D. N. Shubin, E. M. Lobov, E. O. Lobova and N. A. Kandaurov (2021). A Device for Processing a Wideband Signal of the HF Waveband Using a Digital Filter Bank. *2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2021, pp. 1-9, doi: 10.1109/SYNCHROINFO51390.2021.9488356.
60. T. Karp, N.J. Fliege. Modified DFT Filter Banks with Perfect Reconstruction. *IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing*, vol. 46, 11. Pp. 1404-1414, DOI: 10.1109/82.803480
61. R. D. Koilpillai, P. P. Vaidyanathan (1992). Cosine-Modulated FIR Filter Banks Satisfying Perfect Reconstruction // *IEEE Transactions on Signal Processing*. Vol. 40. #4. Pp. 770-783.
62. N. A. Kandaurov, E. M. Lobov (2016). The estimation of the probabilistic characteristics of the algorithm for detecting a series of noise-like signals in a broadband ionospheric channel. *Systems of Signal Synchronization, Generating and Processing in Telecommunications*. Vol. 7. No. 1. Pp. 30-32.
63. V. V. Vityazev (2017). Multi-rate signal processing. Moscow: Hotline – Telecom. 336 p.
64. Software module for detecting and receiving wideband phase-shift keyed signals with an automatic compensator for dispersion distortion / N.A. Kandaurov [and others]. Certificate of state registration of a computer program No. 2018617993 dated 07/05/2018.
65. E. I. Kuli , A. P. Trifonov (1978). The estimation of signals parameters against the background of interference. Moscow: Soviet Radio. 296 p.

#### INFORMATION ABOUT AUTHORS:

**Sergey S. Adjemov**, Doct. of. Sc., professor, Moscow, Russia

**Evgeniy M. Lobov**, Cand. of. Sc., docent, head of research laboratory 4806, SRD MTUCI, lobov@srd.mtuci.ru, Moscow, Russia

**Nikolai A. Kandaurov**, Cand. of. Sc., head of research laboratory 4808, SRD MTUCI, jet1992@yandex.ru, Moscow, Russia

**Elizaveta O. Lobova**, minor researcher research laboratory 4803, SRD MTUCI, lizabeth2@mail.ru, Moscow, Russia

**Vladislav I. Lipatkin**, engineer SRD MTUCI, lipatkin.24@gmail.com, Moscow, Russia

---

**For citation:** Adjemov S.S., Lobov E.M., Kandaurov N.A., Lobova E.O., Lipatkin V.I. Algorithms of estimating and compensating the dispersion distortions of wideband signals in the HF channel. *H&ES Reserch*. 2021. Vol. 13. No. No 5. P. 57-74. doi: 10.36724/2409-5419-2021-13-5-57-74 (In Rus)



doi: 10.36724/2409-5419-2021-13-5-75-85

# ОБНАРУЖЕНИЕ СТЕГОСИСТЕМ, ИСПОЛЬЗУЮЩИХ ПОГРУЖЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОНТУРЫ ИЗОБРАЖЕНИЯ

**КОРЖИК**

**Валерий Иванович<sup>1</sup>**

**НГУЕН**

**Зуи Кыонг<sup>2</sup>**

**ДАНЬШИНА**

**Арина Викторовна<sup>3</sup>**

## АННОТАЦИЯ

**Введение:** общеизвестно, что использование стегосистем повышает информационную безопасность хранения и передачи конфиденциальной информации, обеспечивая скрытие содержания и сам факт присутствия засекреченных данных в "невинных" покрывающих объектах, важнейшими из которых являются, изображения, звуковые и текстовые файлы, интернет-протоколы. Стегосистема используется не только государственными структурами, но и в бизнес обществе для обеспечения организационной или технической конфиденциальности. С другой стороны, является актуальной и технология обнаружения стегосистем, поскольку это позволяет организациям и компаниям защитить секретную информацию от ее утечки во внешний контур, как это делается обычно в системе Data Leakage Prevention. **Цель исследования:** целью является исследование методов обнаружения перспективной стегосистемы с погружением конфиденциальной информации в контуры неподвижного изображения с градациями серого. **Результаты:** описан метод нахождения контуров изображения и алгоритм погружения в них информации, проведена оценка объема вложенной информации, а также возможности обнаружения вложения визуальным и гистограммными методами. В качестве более эффективного метода обнаружения был использован подход, основанный на тестах псевдослучайности. Результаты эксперимента убедительно показали, что данный метод стегоанализа имеет преимущество перед традиционными методами обнаружения стегосистем, особенно, если он сочетается с техникой Support Vector Machine. **Обсуждение:** однако, при вложении информации лишь в некоторую часть пикселей по стегоключу, рассмотренный метод стегоанализа дает лишь небольшие улучшения обнаруживаемости, что говорит о достаточно высокой стойкости стегосистем с вложением в контуры изображения.

## Сведения об авторах:

<sup>1</sup> д.т.н., профессор, почетный профессор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, val-korzhih@yandex.ru

<sup>2</sup> аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А.Бонч-Бруевича

<sup>3</sup> студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

**КЛЮЧЕВЫЕ СЛОВА:** стегосистема, контуры изображения, стегоанализ, тесты на псевдослучайность, метод опорных векторов.

---

**Для цитирования:** Коржик В.И., Нгуен З.К., Даньшина А.В. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 75-85. doi: 10.36724/2409-5419-2021-13-5-75-85

## Ведение

Общеизвестно, что использование стегосистем повышает информационную безопасность хранения и передачи конфиденциальной информации. Действительно, в отличие от криптографии, стегосистемы (СГ) обеспечивают скрытие не только содержания, но и самого факта присутствия конфиденциальных данных в «невинных» покрывающих объектах (ПО), важнейшими из которых являются, изображения, звуковые и текстовые файлы, интернет-протоколы [1].

Помимо очевидного использования СГ государственными структурами, в последнее время такая технология используется и в бизнес сообществе для обеспечения организационной или технической конфиденциальности. С другой стороны, является актуальной и технология обнаружения СГ, поскольку это позволяет организациям и компаниям защитить конфиденциальную информацию от ее утечки во внешний контур, как это делается обычно в системе Data Leakage Prevention (DLP).

Практическая важность, рассмотренных выше задач, стимулирует интенсивную разработку СГ и методов их обнаружения при помощи стегоанализа (СГА). К настоящему времени опубликовано множество научных работ, посвященных исследованию данных направлений, среди которых следует отметить фундаментальную монографию [1], а также монографии, описывающие последние достижения в данной области [2,3].

Как было отмечено в [1], наиболее популярными ПО для использования СГ являются неподвижные изображения (цветные или с градациями серого), поскольку их использование в качестве носителей скрытой информации, например, в электронной почте, выглядит наиболее естественным. Ко всем СГ предъявляются такие очевидные требования, как сложность их обнаружения нелегитимными пользователями, сохранение высокого качества ПО после вложения дополнительной информации и максимизация объема вложения (для заданного объема ПО). Дополнительным требованием является сложность процесса обнаружения. Очевидно, что возможен «обмен» между определенными выше требованиями. Так стойкость к обнаружению может быть повышена, за счет уменьшения объема вложения и наоборот.

Что же касается требований к СГА, то они могут быть описаны парой вероятностей:  $P_m$  – пропуск СГ (то есть решение СГА об отсутствии СГ, в то время, как, в действительности СГ присутствует) и  $P_{fa}$  – вероятность ложного обнаружения СГ (то есть решение СГА о присутствии СГ, в то время, как в действительности СГ отсутствует в тестируемом объекте). Здесь также возможен «обмен» между этими вероятностями, что описывается, так называемой ROC – кривой [1,2].

В научно-технической литературе приводится много различных методов построения СГ, например, таких как: СГ с вложением в наименьшие значащие биты (СГ-НЗБ), СГ с рандомизированным вложением в НЗБ ( $\pm 1$  СГ-НЗБ), с использованием широкополосных сигналов (СГ-ШПС) [4], лингвистические стегосистемы (СГ-Л), с адаптивным квантованием (СГ-АК), с вложением в сканированные изображения (СГ-С), а также, предложенная недавно СГ в каналах с шумом (СГ-Ш) [2]. К сожалению, только СГ-Л и СГ-Ш мо-

гут претендовать на абсолютную необнаруживаемость СГ, однако они могут быть использованы лишь при выполнении особых условий (наличия ПО в виде текста, весьма малые объемы вложения или присутствие шумов в каналах обнаружения СГ).

Поэтому, в большинстве практические рекомендации для СГ систем стремятся обеспечить, по крайней мере,  $P_m$ ,  $P_{fa}$  (или их полной вероятности ошибки  $P_e = ((P_m + P_{fa})/2)$  близких к  $1/2$ .

В последнее время активно предлагается использовать для вложения – вложение в контуры изображения (СГ-К). Поэтому в настоящей работе была выбрана для исследования обнаружения именно такая востребованная СГ.

Ниже описывается метод построения с вложением в контуры СГ, так же оценивается эффективность обнаружения данной СГ такими традиционными методами стегоанализа, как визуальный и гистограммный. Подробно описывается универсальный метод обнаружения на основе использования NIST-тестов. Заключение формулирует основные результаты работы и указывает на возможные перспективы дальнейших исследований в данном направлении.

## Описание метода построения стегосистемы СГ-К с вложением информации в контуры неподвижного изображения с градациями серого.

Наиболее популярным (но нестойким к обнаружению) алгоритмом вложения информации в неподвижные изображения с градациями серого, является метод вложения в НЗБ, то есть удаление наименьшего значимого бита каждого пикселя изображения и замена его на бит конфиденциальной информации:

$$C_w(n) = \sum_{i=0}^{L-1} C_i(n) \cdot 2^{i-1} + b(n), \quad (1)$$

где  $C_i(n) \in (0,1)$ ,  $i = 1, \dots, L$  – биты, описывающие яркость  $n$ -го пикселя изображения,  $L$  – количество бит для представления яркости каждого пикселя (типично  $L = 8$ ),  $b(n)$  – бит конфиденциальной информации, вложенный в  $n$ -ый пиксель,  $C_w(n)$  – значение яркости  $n$ -го пикселя после вложения. (Заметим, что данный алгоритм легко обобщается и на цветные неподвижные изображения формате RGB, когда такие же вложения производятся только в один голубой цвет [1]).

Расширением метода СГ-НЗБ является вложение не в каждый пиксель изображения, а лишь в некоторые пиксели, выбираемые по стегоключу, известному лишь легитимным пользователям, но не стегоаналитику.

Тогда, с точки зрения стегоаналитика, можно считать, что вложение в каждый пиксель производится лишь с известной ему вероятностью «Р» и «невложение» с вероятностью « $1 - P$ ».

Однако, экспериментальные исследования показали, что не все пиксели одинаковы с точки зрения возможности обнаружения вложения, а именно – менее всего подвержены обнаружению пиксели, лежащие на контурах изображения. Определение «контуров» изображения интуитивно очевидно – это те части изображения, где происходят резкие скачки яркости между соседними пикселями изображения.



Используя, отмеченную ранее особенность обнаружения СГ, можно производить вложение не во все пиксели изображения, а лишь в те пиксели, которые лежат на контурах или в более общем виде, вкладывать в контурные пиксели  $k_e > 1$  бит информации, тогда как в «не контурные» (сглаженные) пиксели  $k_s = 1$  бит информации.

Очевидно, что для построения такой СГ необходимо, прежде всего, построить алгоритм выделения контуров изображения, причем такой, который обеспечивает сохранение контуров до и после вложения, чтобы избежать ошибок при извлечении вложенной информации. В настоящее время разработано несколько методов выделения контуров изображения такими авторами как: Robert, Sobel [5], Prewitt [6], а также наиболее эффективный метод Canny [7], основанный на использовании гауссовского фильтра. В настоящей работе был использован именно последний метод выделения контуров изображения.

На рисунке 1 показана общая схема погружения информации в контуры изображения.



Рис. 1. Общая схема погружения для СГ-К

Эта схема, как видно, состоит из двух этапов: первый приводит к выполнению погружения, второй – контроль, подтверждающий сохранение контура после погружения.

Рассмотрим механизм погружения информации, который можно назвать расширенным НЗБ, поскольку в каждый пиксель, лежащий на контуре, вкладывается не один (как в простом НЗБ), а несколько бит секретной информации. Для простоты, будет рассмотрено изображение в градациях серого (когда яркость каждого пикселя принимает одно из 256 значений и поэтому представляется цепочкой из 8-ми бит). Зададим параметр  $p$ , который определяет сколько бит может быть изменено во время вложения, причем типичное  $p = 4$ . Эти  $p$  бит перед обнаружением контура устанавливаются равными нулю. Тогда количество неизменных бит каждого пикселя будет равно:

$$q = 8 - p, \quad (2)$$

Погружение выполняется при помощи использования оператора замены  $k$  НЗБ:

$$y' = y \oplus_k m, \quad (3)$$

где  $y$  – значение яркости пикселя до погружения;  $k = k_e$ , если  $y$  находится на контуре и  $k = k_s$ , если пиксель принадлежит сглаженной области, причем  $k_e$  больше, чем  $k_s$ ;  $p = k_e + 1$ ;  $m$  – секретное сообщение;  $y'$  – полученное значение стего-пикселя после внедрения  $k$  бит;  $\oplus_k$  – обозначает оператор замещения, который встраивает  $k$  бит в  $k$  НЗБ.

Предположим, что  $k$  бит погружается в каждый пиксель изображения. Следующие шаги полностью определяют процедуру вложения:

**Шаг 1:** найдем пиксели изображения  $S$  с обнулением  $p$  бит, лежащие на контуре:

$$S = \{I'_{ij} \mid I'_{ij} = I_{ij} \oplus_p '0..0', (p \text{ нулевых бит})\}, \quad (4)$$

где  $I_{ij}$  – значение пикселя  $(i, j)$  покрывающего изображения;  $p$  – количество бит, которые могут быть изменены во время вложения.

**Шаг 2:** модификация пикселя:

$$s = y \oplus_p '0..0', \quad (5)$$

**Шаг 3:** вычисление:

$$y_1 = y \oplus_k m, \quad (6)$$

**Шаг 4:** если  $|y - y_1| > 2^{k-1}$ , тогда вычислить:

$$y_2 = \begin{cases} y_1 + 2^k, & \text{если } |y_1 + 2^k - y| < |y_1 - 2^k - y| \\ y_1 - 2^k & \text{иначе перейти к шагу 5} \end{cases}, \quad (7)$$

Иначе  $y_{stego} = y_1$ .

**Шаг 5:** если  $y_2 \oplus_p '0..0' = s$ , тогда  $y_{stego} = y_2$ . Иначе  $y_{stego} = y_1$ .

На рисунке 2 приведены примеры реализации метода погружения информации для десяти ПО изображений, размером – 512x512, форматом расширения - .bmp, при некоторых параметрах:  $p = 3$ ,  $k_e = 2$ ,  $k_s = 1$ .

На рисунке 2а представлены изображения в градациях серого, размером 512x512, без вложения информации, на рисунке 2б продемонстрированы контуры, найденные при помощи оператора Кэнни [7]. На (рис.2в) показаны стего-изображения, полученные при помощи вложения информации в контуры изображений, каждое из которых содержит в себе около 979 КБ секретной информации.

По результатам вложения информации в контур изображения, можно сделать вывод, что при заданных параметрах, «невооруженным взглядом» обнаружить наличие стего-системы невозможно. При этом, выполняется главное условие данного метода, не изменяется контур изображения, а следовательно не возникнет проблем с правильным извлечением информации.

Извлечение вложенной информации выполняется при помощи следующих шагов:

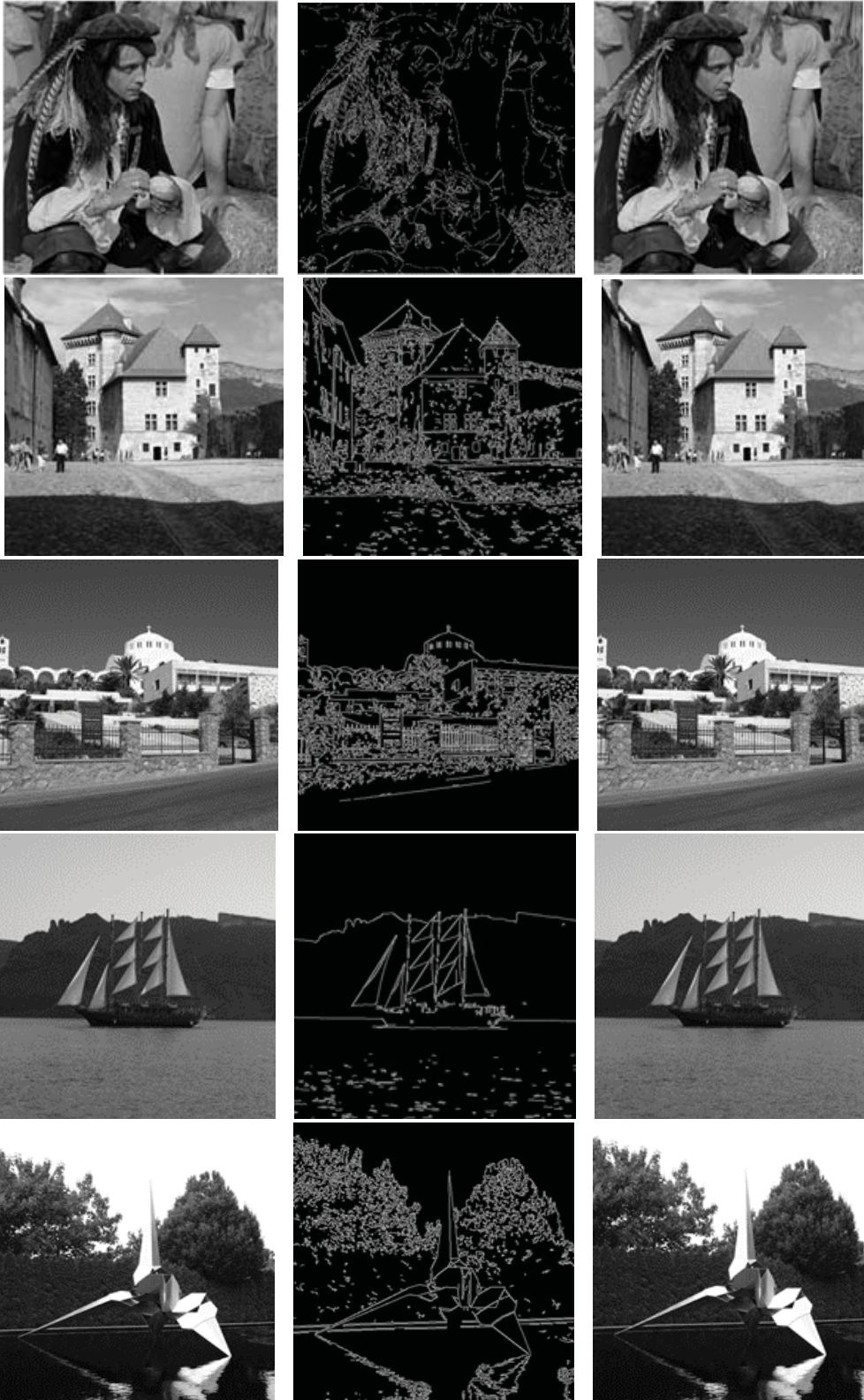
**Шаг 1:** найдем пиксели изображения  $S$  лежащие на контуре, используя известные методы:

$$S = \{I'_{ij} \mid I'_{ij} = I_{ij} \oplus_p '0..0' (p \text{ нулевых бит})\}, \quad (8)$$

где  $I_{ij}$  – значение пикселя  $(i, j)$  стего-изображения;  $p$  – максимальное количество бит, которые могут быть изменены во время вложения.

**Шаг 2:** если  $y$  лежит на контуре, тогда  $k = k_e$ , иначе  $k = k_s$ .

**Шаг 3:** извлечь  $k$ -НЗБ бит из  $y$ .







а)

б)

в)

Рис. 2. Примеры вложения информации в контуры изображений: а) исходное изображение; б) контуры ПО; в) СГ после вложения

Оценим теперь эффективность СГ-К с точки зрения сохранения качества ПО.

Метрики качества, используемые для оценки предлагаемой системы стеганографии, включают пиковое отношение сигнал/шум (PSNR) и среднеквадратическую ошибку (MSE). Большое значение PSNR или малое значение MSE означают хорошее качество изображения. Если PSNR больше 30 дБ, то искажения на изображениях обычно оказываются незаметными.

$$MSE = \frac{\sum M_{r^2} N(T(r,c) - T'(r,c))^2}{M \cdot N}, \quad (9)$$

$$PSNR = 10 \cdot \log_{10} \left[ \frac{R^2}{MSE} \right], \quad (10)$$

В данных формулах,  $T(r,c)$  – это исходное изображение, а  $T'(r,c)$  – результирующее стего-изображение,  $r$  и  $c$  – количество строк и столбцов в матрицах изображений соответственно,  $M \cdot N$  – размер изображения,  $R$  – максимальное отклонение в типе данных входного изображения, можно также сказать, что оно дает максимальное значение интенсивности изображения. Измерение индекса сходства является показателем оценки качества и основывается на вычислении трех терминов, а именно: яркости, контрастности и структурного термина.

Таблица 1 демонстрирует сравнение эффективности предложенного метода (с 2-битным внедрением в контур и однобитного внедрения в «сглаженные» области) с методом НЗБ. Было произведено вложение в 1000 изображений. Изображения имели размер  $512 \times 512$ , с расширением .bmp.

Таблица

Оценка качества 1000 изображений после вложения методами СГ-К и СГ-НЗБ

№ изображения	Среднее значение PSNR при СГ-К, дБ	Среднее значение PSNR при НЗБ, дБ
1-100	48,72	51,140440
100-200	48,8632800	51,140502
200-300	48,	51,140793
300-400	48,	51,142193
400-500	48,	51,141100
500-600	48,	51,141253
600-700	49,	51,139252
700-800	48,	51,139375
800-900	48,	51,140557
900-1000	48	51,140676
итог	48,7534917	51,140614

Из полученных результатов, можно сделать вывод, что рассмотренные методы дают хорошее качество изображения после вложения информации. Хотя, из табл. 1 видно, что среднее значение PSNR несколько выше при вложении в НЗБ, чем при вложении в контур изображения, это происходит из-за того, что при методе НЗБ вкладывается в пиксель только один бит информации, а при контурном вложении вкладывается в контур изображения два бита информации, а в гладкие области один бит.

Следовательно, качество изображения при НЗБ немного выше, чем при вложении в контур, но визуальные различия

между стего-изображениями незаметны.

Скорость вложения, при контурном погружении имеет вид:

$$V_{вл} = \frac{\mu \cdot k_e + \gamma}{\omega}, \quad (11)$$

где  $V_{вл}$  – скорость вложения для контурного погружения,  $\mu$  – количество бит, вкладываемых в контурные пиксели,  $k_e$  – количество изменяемых бит в контуре,  $\gamma$  – количество пикселей, принадлежащих гладкой области,  $\omega$  – количество пикселей изображения. Для 1000 изображений с параметрами:  $p=3$ ,  $k_e=2$ ,  $k_s=1$ , средняя скорость вложения становится равной 1.55, что заметно больше, чем при вложении в НЗБ.

### Оценка эффективности обнаружения СГ-К традиционными методами, используемыми при обнаружении СГ-НЗБ

Рассмотрим сначала популярный метод стегоанализа, основанный на визуальной атаке, который был разработан для обнаружения вложений СГ-НЗБ. Суть данного метода состоит в том, что сначала изображение с градациями серого преобразуется в черно-белое изображение по правилу: яркость каждого пикселя, имеющую НЗБ = 1 преобразуется в яркость, соответствующую белому пикселю, а при НЗБ = 0 в яркость, соответствующую черному пикселю. Далее полученное черно-белое изображение представляется для визуального восприятия.

Тогда если в исследуемом изображении нет вложения, то на вновь полученном черно-белом изображении будут видны некоторые контуры исходного изображения. Если же исследуемое изображение содержит вложение, то новое черно-белое изображение будет выглядеть как шумовое поле. (Особенно при шифровании вложенного сообщения стойким шифром).

На рисунках 3-6 показаны исходные ПО и СК-К после визуального стегоанализа.

Сравнив, покрывающие сообщения после визуальной атаки и стего-изображения после визуальной атаки, сложно заметить какие-либо различия. Это происходит, из-за того, что пикселей, принадлежащих контуру, оказывается больше, чем пикселей, принадлежащий сглаженной области изображений, а обнаружить вложение только в контур, оказывается затруднительно. Следовательно, можно сделать вывод, что обнаружить присутствие стegosистемы визуально достаточно сложно.

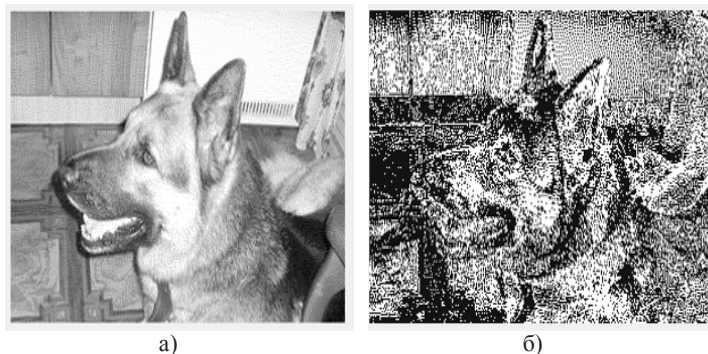


Рис. 3. Покрывающее сообщение:  
а) до атаки; б) после визуальной атаки



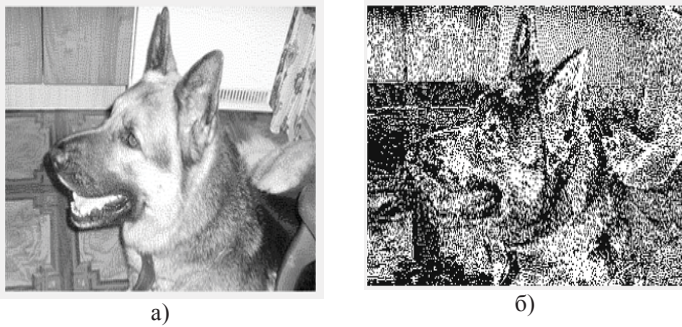


Рис. 4. Стего-изображение: а) до атаки; б) после визуальной атаки

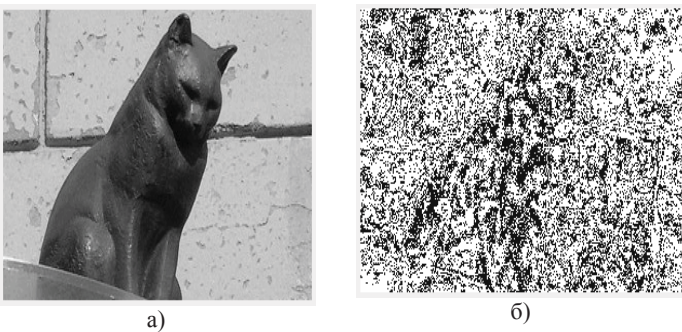


Рис. 5. Покрывающее сообщение: а) до атаки; б) после визуальной атаки

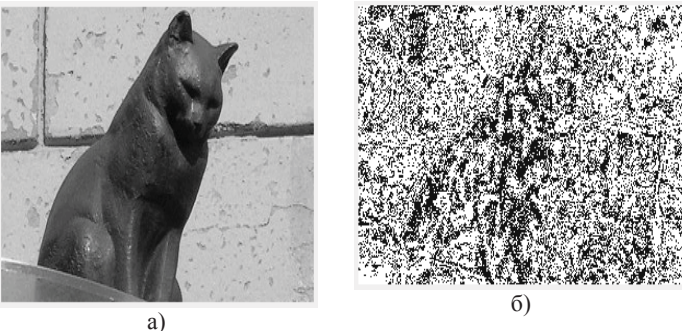


Рис. 6. Стего-изображение: а) до атаки; б) после визуальной атаки

Второй метод, используемый для обнаружения СГ-НЗБ – это, так называемая, *гистограммная атака*, описанная в [2]. Для выполнения этой атаки сначала необходимо произвести вычисление величины:

$$\chi^2 = \frac{\sum_{j=1}^{L-1} (V(2j) - V(2j+1))^2}{2(V(2j) + V(2j+1))} \quad (12)$$

где  $V(j) = \frac{\#\{n \in (1, 2, \dots, N) : (C(n) = j)\}}{N}$ ,  $j = 1, 2, \dots, L$  – гистограмма изображения  $C(n)$ ,  $N$  – общее количество пикселей изображения,  $L$  – количество бит для представления яркости каждого пикселя. Далее производится сравнение величины  $\chi^2$  с некоторым, заранее выбранным, порогом  $\lambda$ . Если  $\chi^2 \leq \lambda$ , то принимается решение о присутствии СГ, а если  $\chi^2 > \lambda$ , то об отсутствии СГ.

В таблице 2 приведены экспериментальные значения  $\chi^2$  для 5 различных стего-изображений с вложением, с помощью СГ-К.

Таблица 1

Значение  $\chi^2$  при вложении методом СГ-К

№ изображения	Значение $\chi^2$ для ПО	Значение $\chi^2$ для СГ-К
1	5821	58476
2	6000	58476
3	5693	55853
4	5958	58449
5	5992	58552

Из данных таблицы 2 видно, что при вложении информации в контур, методом СГ-К, величины  $\chi^2$  для ПО мало отличаются, от значений  $\chi^2$  для стего-изображений. Следовательно, можно сделать вывод, что с помощью гистограммной атаки СГ-К обнаружить затруднительно.

Третий метод для обнаружения СГ-НЗБ – это так называемый *парновыборочный анализ* (далее ПВА) [2].

Рассмотрим данный СГА применительно к методу вложения информации в контур изображения. Предположим, что вложение производилось во все пиксели, то есть  $P=1$ .

Результатом данной атаки является оценка доли вложения –  $P$ . Экспериментальные результаты исследований для пяти изображений при вложении методом СГ-К представлены в (табл. 3).

Таблица 2

Экспериментальные результаты расчета  $P$  по методу ПВА

№ изображения	Оценка доли вложения $P$
1	0,0000
2	
3	
4	0,000
5	

Как видно из таблицы 3, при использовании метода вложения СГ-К, ПВА также не позволяет обнаружить наличие скрытой информации.

Полученные результаты говорят о том, что рассмотренные методы стегоанализа не могут быть эффективно использованы для обнаружения СГ-К, следовательно, необходим новый метод СГА.

### Обнаружение стегосистем при помощи универсального метода, основанного на NIST-тестах

Любая стегосистема, претендующая, хотя бы немного на сложность ее обнаружения, предполагает шифрование сообщений, погружаемых в ПО, стойким шифром. Действительно, во-первых, при известном методе извлечения, стегоаналитик, может считать сообщение и принять решение о присутствии стеговложения, если извлеченные пиксели (или данные) будут смысловыми. (Если же извлечение информации будет требовать секретного стегоключа, то стегоаналитик может попытаться отследить его, например, методом перебора).

Во-вторых, хотя иногда применение стеганографии и объясняется заменой ею криптографии [1], но такая цель кажется весьма сомнительной, поскольку знание алгоритма извлечения информации, будет тогда приводить не только к обнаружению факта секретного вложения, но и к «чтению» вложенной информации, что, как правило, еще более опасно, чем только обнаружение вложения. Поэтому, будем далее предполагать, что перед вложением в ПО, сообщения подвергаются стойкому шифрованию. Тогда возникает следующая идея выполнения стегоаналитического алгоритма:

- извлечь из тестируемого объекта предполагаемую криптограмму, используя известный или даже известный лишь частично, алгоритм извлечения;
- проверить извлеченную последовательность на псевдослучайность, используя стандартные NIST-тесты;
- принять решение об обнаружении СГ, если все NIST-тесты проходят, и решение об отсутствии СГ, в противоположном случае.

Обобщением такого метода обнаружения является выбор некоторого порога, который должен быть превышен количеством пройденных тестов или использованием техники опорных векторов (Support Vector Machine – SVM), которые обсуждаются далее.

Общеизвестно [8], что криптограмма для стойких шифров должна удовлетворять всем тестам на псевдослучайность. С другой стороны, последовательность извлеченная из ПО, которая не является криптограммой, не будет очевидно удовлетворять большинству тестов на псевдослучайность. Однако последнее утверждение требует проведения экспериментальной проверки. Впервые данный подход был проверен и опубликован в работе [9] применительно к стеганограммам с вложением информации в НЗБ, а также распространен на матричное вложение, использующее коды Хэмминга.

В настоящей работе рассмотрено распространение этого алгоритма для обнаружения стегосистем с вложением информации в контуры неподвижных изображений. Такая задача представляет особый интерес, поскольку, во-первых, СГ с вложением в контуры изображения считаются в настоящее время особенно перспективными, и, во-вторых, они как показано в Разделе 3, настоящей работы, не поддаются обнаружению при использовании традиционных методов.

В таблице 4 представлен список названий 15 стандартных NIST тестов, заимствованный из [10].

Для эксперимента был выбран метод вложения в контуры неподвижного изображения с параметрами:  $p=3$ ,  $k_e=2$ ,  $k_s=1$  и для шифрования был использован стойкий шифр ГОСТ – 28147-89 [2]. Для шифрования было выбрано 15 различных изображений из базы изображений размером 512x512.

Результаты тестирования показаны в таблице 5. Из данной таблицы видно, что СГ проходят абсолютное большинство тестов.

В таблице 6 показаны результаты тестирования для двоичных последовательностей, полученных из 15-ти различных изображений без вложений, извлеченных из конура (с известными параметрами  $p$ ,  $k_e$ ,  $k_s$ ).

Таблица 3

Название 15-ти стандартных NIST-тестов на псевдослучайность

№ test	Title of test
1	The frequency test
2	Frequency test within a block
3	The runs test
4	Tests for the longest-run-of-ones in a block
5	The binary matrix rank test
6	The discrete Fourier transform (spectral) test
7	The non-overlapping template matching test
8	The overlapping template matching test
9	Maurer’s “Universal Statistical” test
10	The linear complexity test
11	The serial test
12	The approximate entropy test
13	The cumulative sums (cusums) test
14	The random excursion test
15	The random excursions variant test

Таблица 4

Результаты прохождения 15-ти СГ с вложением информации после шифрования ГОСТ – 28147-89

Изобр. Тесты	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															

Таблица 5

Результаты тестирования для 15-ти различных последовательностей, извлеченных из ПО без вложения

Seq. Test	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															

Видно, что таблицы 5 и 6 коренным образом отличаются друг от друга. Однако, чтобы получить «количественное» подтверждение эффективности данного метода обнаружения, было протестировано 1000 различных изображений для каждого из тестов и в таблице 7 представлены результаты расчетов вероятностей ошибок  $P_m$  (вероятность пропуска СГ),  $P_{fa}$  (вероятность ложной тревоги) и  $P_e = \frac{1}{2}(P_m + P_{fa})$ , рассчитанные для, описанного ранее, алгоритма обнаружения на основе использования NIST-тестов. Видно, что полная вероятность ошибки  $P_e$  минимизируется при выборе порога 13 и получается равной 11,5 %.

Таблица 6

Вероятности ошибок  $P_m$ ,  $P_{fa}$ ,  $P_e$  (в %), в зависимости от выбора порога прохождения числа тестов

Threshold	$P_m$	$P_{fa}$	$P_e$
0	0	10	50
1	0	96,	48,2
2	0	89,	44,55
3	0	8	42
4	0	74,	37,2
5	0	67,	33,65
6	0	54,	27,45
7	0	44,	22,25
8	0	36,	18,2
9	0,1	32	16,05
10	0,1	28,7	14,4
11	0,2	25,4	12,8
12	1,3	23,5	12,4
13	3,4	19,6	11,5
14	27,3	13,5	20,4
15	40,4	8,1	24,25

Для того, чтобы уменьшить полную вероятность ошибки обнаружения  $P_e$ , был рассмотрен метод классификации по правилу опорных векторов с гауссовским нелинейным ядром  $k(x, x') = \exp(-\gamma \|\bar{x} - x'\|^2)$ .

Данный метод был предложен в работе [1] и подробно рассмотрен в [2]. Этот метод использует процедуру предварительного обучения на статистике 1000 ПО без вложений и 1000 СГ с вложением по контуру. После выполнения предварительной процедуры обучения, вырабатывается решающая функция, по которой и производится тестирование объектов СГ или ПО не входивших в число объектов тестирования.

Результаты тестирования по оценке псевдослучайности, использующей NIST-тесты и технику SVM, показана в (табл.8), где были также оптимизированы параметры SVM  $\gamma = 32$  и  $C = 1$ .

Таблица 7

Оценки вероятностей ошибок при тестировании на основе NIST-тестов с использованием техники SVM

SVM параметры	$\gamma = 32; C = 1$
$P_{fa}$	13,2
$P_m$	2,4
$P_e$	7,8

Сравнивая результаты таблиц 7 и 8 видим, что переход к технике SVM показывает некоторое небольшое (но важное для стегоанализа) преимущество последнего метода. (Интересно отметить, что использование методов распознавания классов при помощи процедуры обучения (как в SVM) иногда трактуется в литературе как элемент «искусственного интеллекта», поскольку решающая функция в этом случае не может данное заранее спрогнозирована).

Для улучшения необнаруживаемости СГ, даже при использовании погружении информации в контуры изображения, можно дополнительно попытаться выполнить вложение в часть пикселей по стегоключу.

В таблице 9 представлены результаты такого эксперимента для 3-х значений вероятностей вложения в пиксели контура  $p=0,9; 0,5; 0,1$ .

Таблица 8

Вероятности ошибок при обнаружении на основе NIST-тестов стegosистем с вложением в контур с вероятностями ошибок  $p = 0,9; 0,5; 0,1$ , в зависимости от величины порога числа прохождений тестов

p	0,9			0,5			0,1		
	$P_m$	$P_{fa}$	$P_e$	$P_m$	$P_{fa}$	$P_e$	$P_m$	$P_{fa}$	$P_e$
0	0	100	50		100	50		100	50
1	0	96,	48.2	0	96,4	48.2	0	96,4	48.2
2	0	89,1	44.55	0.2	89,1	44.65	5.4	89,1	47.25
3	0.	84	42.05	8.1	84	46.05	13.2	84	48.6
4	0.2	74,4	37.3	13.8	74,4	44.1	22.8	74,4	48.6
5	0.	67,3	34.05	17.3	67,3	42.3	30.3	67,3	48.8
6	1.	54,9	28.15	21.6	54,9	38.25	41.3	54,9	48.1
7	1.	44,5	23.15	24.6	44,5	34.55	51.1	44,5	47.8
8	2.	36,4	19.55	29.5	36,4	32.95	59.3	36,4	47.85
9	5	32	18	34.3	32	33.15	63.4	32	47.7
10	6.9	28,7	17.8	38.9	28,7	33.8	65.8	28,7	47.25
11	8.8	25,4	17.1	43.8	25,4	34.6	69.3	25,4	47.35
12	12	23,5	17.75	50.4	23,5	36.95	73	23,5	48.25
13	15.4	19,6	17.5	57.3	19,6	38.45	77.7	19,6	48.65
14	37.1	13,5	25.3	71	1	42.25	85	13	49.25
15	50.7	8,1	29.4	80.7	8,1	44.4	89.9	8,1	49

Из данной таблицы видно, что даже при минимизации выбора порога, полная вероятность ошибки  $P_e=47\%$ , что близко к тривиальному методу обнаружения СГ случайным угадыванием. Применение метода обнаружения с использованием SVM, позволяет, как показали наши эксперименты лишь несколько уменьшить эту вероятность ошибки до  $P_e=35\%$ , хотя такую величину также нельзя назвать удовлетворительной.

### Заключение

В настоящей работе исследовано обнаружение перспективной стegosистемы при помощи недавно предложенного метода, основанного на использовании NIST-тестов. Результаты эксперимента убедительно показали, что данный метод обнаружения имеет преимущество перед традиционными методами обнаружения стegosистем с вложением в НЗБ.

Предложенный подход оказывается особенно эффективным, если NIST-тестирование сочетается с техникой SVM.



При вложении информации лишь в некоторую часть пикселей по стегоключу, рассмотренный метод дает лишь небольшие улучшения обнаруживаемости, что говорит о достаточно высокой стойкости стegosистем с вложением в контуры изображения. Еще одним методом защиты стegosистем от обнаружения, использующего NIST-тестирование, является специальное преобразование криптограмм перед их вложением в ПО, которое подробно исследовано в работе [11].

### Литература

1. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., И.А. Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография. СПб.: СПбГУТ, 2016. 18 с.
2. Анфиногенов С.О., Кочкарев А.И., Федянин И.А., Жувикин А.Г., Флакман Д.А., Алексеев В.Г. Цифровая стеганография и цифровые водяные знаки. Часть 2. Цифровая стеганография. СПб.: СПбГУТ, 2017. 198 с.
3. Яковлев В.А. Основы криптографии: учебное пособие. СПб: ИЦ Интермедия, 2016. 296 с.
4. Oswal S., Singh A., Kumari K. Deflate Compression Algorithm // International Journal of Engineering Research and General Science. 2016. Pp. 430-436.
5. Dadgostar H. Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB // Journal of information security and applications. 2016. Pp. 94-104.
6. Ахрамеева К.А. Обнаружение видео стegosистем универсальным методом, основанным на использовании NIST-тестов // Труды учебных заведений связи. 2020. С. 70-76.
7. Kadhim I. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research // Neurocomputing. 2019. Pp. 299-326.
8. Грибунин В. Г., Оков И. Н., Туринцев И.В. Цифровая стеганография. М.:СОЛОН-Пресс, 2016. 262 с.
9. Marton K. On the interpretation of results from the NIST statistical

test suite // Science and Technology. 2016. №. 1. Pp.18-32.

10. Герлинг Е.Ю., Ахрамеева К.А. Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019. № 3 С. 51-58.
11. Nie S.A., Abel A., Sulong G., Ali R. The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image // International Journal of Electrical and Computer Engineering. 2019. Pp. 5218-5226.
12. Nguyen C., Fedyanin I., Morales-Luna G. Side attacks on stegosystems executing message encryption previous to embedding // Journal of Information Hiding and Multimedia Signal Processing. 2020. Pp. 44-57.
13. Ахрамеева К.А., Герлинг Е.Ю., Радынская В.Е. Автоматизация визуального метода на НЗБ // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1. Естественные и технические науки. 2020. № 1.С. 42-45.
14. Korzhik V., Fedyanin I., Morales L. Steganalysis based on statistical properties of the encrypted messages // Lecture Notes in Computer Science. 2017. №10446. Pp.288-298.
15. Guillermo M. Cipher Modification Against Steganalysis Based on NIST Tests // Conference of Open Innovations Association. Москва, 2019. Pp.179-186.
16. Korzhik V. Steganalysis based on statistical properties of the encrypted messages // International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, Cham, 2017. Pp. 288-298.
17. Afsari F., Eslami, E. Interval-valued intuitionistic fuzzy generators: Application to edge detection // Journal of Intelligent & Fuzzy Systems. 2016. №. 3. Pp. 1309-1324.
18. Wang Y. The LSB-based high payload information steganography // International conference on mechatronics, electronic, industrial and control engineering. Atlantis Press, 2017. Pp. 776-9.
19. Wu HC, Wu NI, Tsai CS, Hwang MS. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IET Image Process, 2016. Pp. 611-15.
20. Park YR, Kang HH, Shin SU, Kwon KR. A steganographic scheme in digital images using information of neighboring pixels // Springer Berlin Heidelberg. 2018. №2. Pp. 962-7.

## DETECTION OF STEGOSYSTEM USING EMBEDDING INTO CONTOURS OF IMAGES

**VALERY I. KORZHIK**

St-Petersburg, Russia, val\_korzhik@yandex.ru

**ZUE K. NGUEN**

St-Petersburg, Russia

**ARINA V. DANSHINA**

St-Petersburg, Russia

### ABSTRACT

**Introduction:** it is well known that the use of stegosystems increases the information security of storage and transmission of confidential information, ensuring the concealment of the content and the very fact of the presence of classified data in "innocent" covering objects, the most important of which are images, sound and text files, and Internet protocols. The stegosystem is used not only by government agencies, but also in the business community to ensure organizational or technical confidentiality. On the other hand, the technology of detecting stegosystems is also relevant, since it allows organizations and companies to protect classified information from its leakage into the external circuit, as is usually done in the Data Leakage Prevention system. **Purpose of the study:** the purpose is to study methods for detecting a promising stegosystem with the immersion of con-

**KEYWORDS:** stegosystems, image contour, stegoanalysis, pseu dorandom NIST tests, SVM technique.

fidential information into the contours of a still image with grayscale. **Results:** a method for finding image contours and an algorithm for immersing information in them are described, an assessment of the amount of embedded information, as well as the possibility of detecting an embedding by visual and histogram methods, is carried out. An approach based on pseudo-randomness tests was used as a more efficient detection method. The results of the experiment convincingly showed that this method of steganalysis has an advantage over traditional methods of detecting stegosystems, especially if it is combined with the Support Vector Machine technique. **Discussion:** however, when information is embedded only in a certain part of pixels using a stegokey, the considered steganalysis method gives only small improvements in detectability, which indicates a fairly high resistance of stegosystems with embedding in image contours.



## REFERENCES

1. Korzhik V.I., Nebaeva K.A., Gerling E.Yu., Dogil PS, I.A. Fedyanin I.A. (2016). Digital steganography and digital watermarks. Part 1. Digital steganography. SPb.: SPbGUT. 18 p.
2. Anfinogenov S.O., Kochkarev A.I., Fedyanin I.A., Zhuvikin A.G., Flaksman D.A., Alekseev V.G. (2017). Digital steganography and digital watermarks. Part 2. Digital steganography. SPb.: SPbGUT. 198 p.
3. Yakovlev V.A. (2016). Fundamentals of Cryptography: A Tutorial. SPb: IC Intermedia. 296 p.
4. Oswal S., Singh A., Kumari K. (2016). Deflate Compression Algorithm. *International Journal of Engineering Research and General Science*. Pp. 430-436.
5. Dadgostar H. (2016). Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. *Journal of information security and applications*. Pp. 94-104.
6. Akhrameeva K.A. (2020). Detection of video stegosystems by a universal method based on the use of NIST tests. *Proceedings of educational institutions of communication*. Pp. 70-76.
7. Kadhim I. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*. Pp. 299-326.
8. Gribunin V.G., Okov I.N., Turintsev I.V. (2016). Digital steganography. Moscow: SOLON-Press. 262 p.
9. Marton K. (2016). On the interpretation of results from the NIST statistical test suite. *Science and Technology*. No. 1. Pp. 18-32.
10. Gerling E.Yu., Akhrameeva K.A. (2019). Review of modern software using steganography methods. *Economy and quality of communication systems*. No. 3 Pp. 51-58.
11. Nie S.A., Abel A., Sulong G., Ali R. (2019). The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image. *International Journal of Electrical and Computer Engineering*. Pp. 5218-5226.
12. Nguyen C., Fedyanin I., Morales-Luna G. (2020). Side attacks on stegosystems executing message encryption previous to embedding. *Journal of Information Hiding and Multimedia Signal Processing*. Pp. 44-57.
13. Akhrameeva K.A., Gerling E.Yu., Radynskaya V.E. (2020). Automation of the visual method at NZB. *Bulletin of the St. Petersburg State University of Technology and Design. Series 1. Natural and technical sciences*. No. 1. Pp. 42-45.
14. Korzhik V., Fedyanin I., Morales L. (2017). Steganalysis based on statistical properties of the encrypted messages. *Lecture Notes in Computer Science*. No. 10446. Pp. 288-298.
15. Guillermo M. (2019). Cipher Modification Against Steganalysis Based on NIST Tests. *Conference of Open Innovations Association*. Moscow. Pp. 179-186.
16. Korzhik V. (2017). Steganalysis based on statistical properties of the encrypted messages. *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, Cham, Pp. 288-298.
17. Afsari F., Eslami, E. (2016). Interval-valued intuitionistic fuzzy generators: Application to edge detection. *Journal of Intelligent & Fuzzy Systems*. No. 3. Pp. 1309-1324.
18. Wang Y. (2017). The LSB-based high payload information steganography. *International conference on mechatronics, electronic, industrial and control engineering*. Atlantis Press. Pp. 776-9.
19. Wu HC, Wu NI, Tsai CS, Hwang MS. (2016). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IET Image Process*. Pp. 611- 15.
20. Park YR, Kang HH, Shin SU, Kwon KR. (2018). A steganographic scheme in digital images using information of neighboring pixels. Springer Berlin Heidelberg. No.2. Pp. 962-7.

## INFORMATION ABOUT AUTHORS:

**Valery I. Korzhik** - PhD, Full Professor of The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, St. Petersburg

**Zue K. Nguyen** - student of The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, St. Petersburg

**Arina V. Danshina** - student of The Bonch-Bruевич Saint-Petersburg State University of Telecommunications, St. Petersburg

---

**For citation:** Korzhik V.I., Nguyen Z.K., Danshina A.V. Detection of stegosystem using embedding into contours of images. H&ES Reserch. 2021. Vol. 13. No. No 5. P. 75-85. doi: 10.36724/2409-5419-2021-13-5-75-85 (In Rus)

doi: 10.36724/2409-5419-2021-13-5-86-95

# ВОПРОСЫ ОЦЕНКИ НАДЕЖНОСТИ СОВРЕМЕННЫХ СИСТЕМ ХРАНЕНИЯ ДАННЫХ ДЛЯ МОБИЛЬНЫХ ДАТА-ЦЕНТРОВ

**КРЮКОВА**

**Елена Сергеевна<sup>1</sup>**

**ТКАЧЕНКО**

**Владимир Владиславович<sup>2</sup>**

**МИХАЙЛИЧЕНКО**

**Антон Валерьевич<sup>3</sup>**

**ПАРАЩУК**

**Игорь Борисович<sup>4</sup>**

## Сведения об авторах:

<sup>1</sup> адъюнкт кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, e.krukova69@yandex.ru

<sup>2</sup> старший инженер в/ч 42915, Москва, Россия, U-429@inbox.ru

<sup>3</sup> адъюнкт кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, katjuha777@inbox.ru

<sup>4</sup> д.т.н., профессор, Заслуженный изобретатель Российской Федерации, профессор кафедры автоматизированных систем специального назначения Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, shchuk@rambler.ru

## АННОТАЦИЯ

**Введение:** проведен обзор в области современных подходов к созданию и совершенствованию методов оценки надежности систем хранения данных мобильных дата-центров, предназначенных для непрерывного предоставления с высоким качеством набора базовых и дополнительных информационных услуг. При этом услуги потребителям предоставляются в любом месте их расположения, где типовые дата-центры решают не только задачи построения информационной инфраструктуры организаций, ведомств и отдельных крупных предприятий, но и задачи, ориентированные на обеспечение информационной безопасности этих инфраструктур. Обобщены и систематизированы цели и задачи систем хранения данных, как технологической основы мобильных дата-центров, особенности архитектур, технологий и условий их построения и функционирования. Изучены и сформулированы показатели надежности систем хранения данных, исследованы роль и место задач оценки надежности. Обоснованы актуальность обеспечения точности и многокритериальности оценки надежности в интересах поддержки принятия решений по проектированию и построению систем хранения данных. Предметом исследования является надежность систем хранения данных, как набора взаимосвязанных компонентов (каналов, коммутаторов, блейд-серверов, дисков, дисковых массивов и библиотек), а также условий проектирования и построения систем такого класса, которые влияют на их надежность. **Цель исследования:** анализ существующих и разработка нового научно-методического аппарата и программных средств оценки надежности систем хранения данных мобильных дата-центров для обеспечения достоверного и многокритериального (с учетом многообразия компонентов и схем взаимодействия) анализа надежности как самих систем хранения, так мобильных дата-центров в целом. Результаты: предложен метод анализа надежности систем хранения данных для мобильных дата-центров, состоящий из ряда последовательно выполняемых этапов. Метод и алгоритм его реализации основан на логико-вероятностном подходе к оценке надежности, является простым в программной реализации и рациональным с точки зрения оперативности и вычислительной сложности. **Практическая значимость:** представленный подход позволяет сформулировать показатели надежности и оценить надежность сложных структур систем хранения данных. Осуществлена практическая программная реализация на языке C++ в среде разработки Visual Studio. Получены результаты вычислительного эксперимента, которые могут служить исходными данными при принятии решения в рамках выбора систем хранения на этапах проектирования, утверждения проекта, замены или обновления систем хранения данных для мобильных дата-центров.

**КЛЮЧЕВЫЕ СЛОВА:** система хранения данных, мобильный дата-центр, надежность, компонент, оценка, метод, алгоритм, структура.

**Для цитирования:** Крюкова Е.С., Ткаченко В.В., Михайличенко А.В., Паращук И.Б. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Научные исследования в космических исследованиях Земли. 2021. Т. 13. № 5. С. 86-95. doi: 10.36724/2409-5419-2021-13-5-86-95

## Введение

Современная эпоха, по праву называемая эрой информационных технологий, позволила решить много общих проблем и частных практических задач, стоявших перед государством, обществом и отдельным человеком. Вместе с тем, эпоха информационных технологий породила и целый ряд новых, уникальных проблем человечества.

Одна из таких проблем – безопасное владение и хранение большого объема такого важного и, безусловно, ценного ресурса, как информация. Причем ценность данного ресурса делает эту проблему актуальной как на государственном уровне, так и на уровне ведомств, организаций и отдельных компаний.

Иными словами, необходимо обладать эффективной стратегией хранения, защиты, совместного доступа и управления самым важным цифровым ресурсом современного информационного общества – данными. Для реализации этой стратегии зарубежные и российские государственные структуры, силовые ведомства, коммерческие организации и частные компании создают специализированные аппаратно-программные объекты, призванные обеспечивать хранение и обработку информации – дата-центры (ДЦ), зачастую называемые в отечественной литературе центрами обработки данных [1-3].

На протяжении последних десяти лет эта отрасль технических знаний и сфера практической деятельности получили большое развитие. Современные ДЦ играют все более значимую роль в информационном пространстве нашей страны в целом, и в информационно-телекоммуникационной среде системы национальной безопасности и обороны, в частности.

Современные ДЦ представляет собой взаимоувязанные по целям и задачам, емкие и мощные информационные системы, предназначенные для организации, обработки и хранения упорядоченного и пополняемого фонда данных, а также для обеспечения оперативного и безопасного доступа к этим данным должностных лиц с помощью специальных средств и алгоритмов поиска [1-5].

Существующие и активно эксплуатируемые ДЦ специального назначения уже сегодня способны обеспечить хранение и обработку громадных массивов оперативных данных, а также предоставить доступ к огромному объему информационных ресурсов. При этом, помимо традиционных задач по обработке и хранению, так называемых, «больших данных», эти системы работают в широком диапазоне информационно-справочных и информационно-поисковых услуг, а их развертывание не требует значительных временных и материальных затрат. При этом они позволяют хранить, обрабатывать и предоставлять должностным лицам данные с требуемым качеством и в требуемом районе размещения этих лиц [1, 5, 6].

Одним из путей развития теории построения и практики применения систем такого класса, направленным на улучшение эффективности их функционирования, повышение степени доступности и расширение номенклатуры предоставления, услуг является создание мобильных ДЦ [7-10].

Мобильный ДЦ (МДЦ) предназначен для непрерывного предоставления с высоким качеством набора базовых и дополнительных информационных услуг. При этом услуги

потребителям предоставляются в любом месте их расположения. Типовые МДЦ, помимо прочего, решают не только задачи построения IT-инфраструктуры организаций, ведомств и отдельных крупных предприятий, но и задачи, ориентированные на обеспечение информационной безопасности этих инфраструктур [11, 12].

Эффективность мобильных дата-центров обусловлена их возможностями – способностью оперативно переместить, установить и развернуть IT-инфраструктуру в отдаленных (часто труднодоступных) районах, способностью к размещению услуг рядом с потребителями, так называемое «приближение к клиенту», возможностью быстрого наращивания мощности (масштабирования) инфраструктуры, удобством использования достоинств МДЦ для выполнения функций резервного центра обработки данных организаций, ведомств и отдельных предприятий [13-15].

Мобильные дата-центры, как и стационарные центры обработки данных, отвечают за информационное обеспечение должностных лиц с точки зрения: моделирования объектов и процессов (например, «модель войсковой операции); прогнозирования событий и угроз; предоставления услуг по хранению информации и ее структурно-лингвистической обработке на удаленных серверах (аналог «облачных» услуг); предоставления поисковых и информационно-справочных услуг, а также базовых вычислительных (расчетно-аналитических) услуг [1-4].

В рамках управления МДЦ, формирования их состава (выбора элементов) и при решении иных сопутствующих задач управления – поиска направлений повышения качества систем такого класса, продолжают оставаться актуальными задачи квалиметрии, т. е., задачи оценки качества и надежности элементов мобильных центров обработки данных и дата-центров в целом. При этом особого внимания заслуживает методология оценки надежности ключевых, определяющих главный функционал, элементов МДЦ — систем хранения данных (СХД).

Основные трудности решения задач оценки надежности СХД для МДЦ обусловлены, среди прочего, отсутствием универсальных методов многокритериального анализа, учитывающих разнообразие свойств, особенности и разнородность параметров надежности СХД, применяемых для современных МДЦ. Не существует методов, позволяющих осуществить обоснованный выбор типа и структуры СХД для МДЦ, методов, учитывающих неопределенность, неполноту и неоднородность исходной информации о надежности различных современных аппаратных и программных средств СХД в составе мобильных комплексов такого класса. Поэтому разработка новых методов оценки надежности СХД для МДЦ, в том числе, при неполной и неопределенной исходной информации, является важной, актуальной задачей.

## Основные технологии хранения данных для мобильных дата-центров

Одним из ключевых требований к современным, хорошо спроектированным МДЦ, является требование по оперативному предоставлению надежных вычислительных ресурсов и ресурсов хранения данных. Именно поэтому одним из основных вопросов является отказоустойчивость систем хра-

нения, как основных элементов МДЦ, т.е. надежность работы как единичных устройств СХД, так и самой системы в целом [16-19].

Под СХД понимают диски, дисковые массивы, ленточные библиотеки, а также каналы передачи данных, обеспечивающие ввод-вывод, хранение и транспортирование информации внутри МДЦ. При этом различают несколько базовых технологий и структур, которые либо применяются, либо могут быть применимы для задач, решаемых мобильными дата-центрами.

Один из возможных вариантов решения данных задач – технология Direct Attached Storage (DAS). Эта технология подразумевает прямое (непосредственное) подключение накопителей к серверу МДЦ или к компьютерам администраторов и пользователей мобильного центра обработки данных. При этом накопители DAS-системы хранения для МДЦ (жесткие диски, ленточные накопители) могут быть как внутренними, так и внешними. Простейший вариант СХД типа DAS можно построить на базе одного диска внутри сервера МДЦ или компьютера администратора центра обработки данных. В рамках этого варианта (DAS-система) построения СХД для МДЦ также возможно техническое решение, основанное на организации внутреннего RAID-массива дисков с использованием RAID-контроллера [19, 20].

Традиционно под СХД типа DAS принято понимать внешнюю стойку или корзину с дисками, которую можно рассматривать как автономную систему хранения МДЦ. Помимо независимого питания, что важно для МДЦ, такие автономные DAS-системы имеют специализированный контроллер (процессор) для управления массивом накопителей центра обработки данных. Как и для стационарных центров, автономные системы хранения типа DAS могут иметь несколько внешних каналов ввода-вывода, что обеспечивает возможность подключения к СХД нескольких рабочих мест МДЦ одновременно.

Основным преимуществом СХД, построенным по технологии DAS, является их небольшая стоимость (по сравнению с другими решениями СХД для МДЦ), простота развертывания и администрирования в рамках мобильных центров обработки данных, а также высокая скорость обмена данными между системой хранения и сервером МДЦ. Благодаря этим преимуществам СХД, построенные по технологии DAS, завоевали большую популярность в сегменте мобильных систем и сетей. К недостаткам относят слабую управляемость, а также неоптимальное расходование ресурсов, так как каждая DAS-система требует подключения выделенного сервера МДЦ. Системы DAS обычно используют при необходимости увеличения дискового пространства одного сервера МДЦ и вынесения его за корпус. Также DAS-системы могут быть применены в качестве СХД для мобильных центров, обрабатывающих большие объемы данных (например, для МДЦ радиоразведки).

На смену DAS-системам в МДЦ постепенно приходят либо универсальные решения с возможностью плавной миграции к системам Network Attached Storage (NAS), поскольку МДЦ могут быть взаимосвязаны в единую сеть, либо системы, предусматривающие возможность их использования как в качестве DAS, так и NAS, и даже в качестве SAN-

систем. Технология NAS предопределяет создание сетевых СХД, непосредственно подключаемые к сети, объединяющей различные МДЦ, точно так же, как и сетевой почтовый сервер, маршрутизатор или любое другое сетевое устройство [16-20].

Системы хранения МДЦ, построенные по технологии NAS, работают с оптимизированной операционной системой, которая свободна от всех «второстепенных» функций, не связанных с обслуживанием файловой системы и реализацией ввода-вывода данных. Поэтому говорят, что СХД на основе NAS имеют оптимизированную по скорости доступа файловую систему. Это одно из важных достоинств NAS-систем с точки зрения их применения в МДЦ – все вычислительные мощности и ресурсы такой системы сконцентрированы только на операциях обслуживания и хранения файлов. Причем конфигурирование NAS-устройств хранения в рамках МДЦ и подсоединение таких устройств представляет собой несложную задачу для администратора мобильного центра. Иными словами, NAS-устройства являются более производительными и менее дорогими.

Еще одним вариантом решения задачи хранения данных, например, в рамках сети, связывающей несколько МДЦ, может быть технология SAN (Storage Area Network) [20]. Это, по сути, сеть хранения данных, технология организации СХД на основе выделенной сети. Это уже не отдельное устройство в структуре МДЦ, а комплексное решение, представляющее собой специализированную сетевую инфраструктуру. Сети, элементами (узлами) которых служат МДЦ, хранение и обработка данных в которых организована по технологии SAN, связывают один или несколько серверов (SAN-серверов) МДЦ с одним или несколькими устройствами хранения данных МДЦ. В таких системах любой SAN-сервер МДЦ получает доступ к любому устройству хранения данных, не загружая при этом ни другие серверы, ни локальную сеть. Это позволяет очень большому числу пользователей МДЦ хранить информацию в одном месте (с быстрым централизованным доступом) и совместно ее использовать.

#### **Обоснование параметров и этапов оценки надежности систем хранения данных для мобильных дата-центров**

С точки зрения обеспечения надежности, к особенностям СХД МДЦ можно отнести:

- эти системы являются сложными техническими комплексами, которые оснащаются разнообразными программными средствами.

- дефекты программного обеспечения могут иметь последствия, аналогичные последствиям, вызванные отказом технических средств, такие как потеря отдельных функций, задержка выполнения функций, искажение информации.

- отказы элементов, компонентов (ветвей) СХД МДЦ могут не проявляться в явном виде и не обнаруживаться визуально. Для обнаружения отказов в СХД МДЦ создаются и могут использоваться специальные средства контроля и диагностики.

Все эти особенности нельзя не учитывать при проведении оценки надежности СХД такого класса. При этом результаты оценки надежности СХД являются исходными



данными для принятия решений по построению МДЦ. Эти результаты будут влиять на обеспечение надежного выполнения функций СХД, т.е., на надежность МДЦ в целом, а также на сохранение производительности мобильных центров обработки данных, под которой понимается способность этих систем преобразовывать требуемые объемы информации в установленные сроки.

Для расчета надежности СХД МДЦ необходимо определить, какие элементы систем хранения и их характеристики необходимо рассматривать. Надежность системы хранения напрямую зависит от надежности входящих в систему элементов. Для оценки надежности системы СХД целесообразно разбить на компоненты (направления, секторы, ветви), представляющие собой каналы передачи данных, обеспечивающие ввод-вывод, хранение и транспортирование информации между дисками, дисковыми массивами и библиотеками СХД. Причем каждому из компонентов (направлений, ветвей) СХД задано требование к качеству обслуживания, определены показатели надежности составляющих СХД МДЦ подсистем.

Совокупность показателей надежности функционирования всех компонентов (направлений, ветвей) СХД МДЦ (включая, среди прочего, надежность подсистем защиты информации в СХД и надежность программного обеспечения), характеризует надежность системы в целом [21-23].

Одним из базовых показателей, характеризующих надежность СХД МДЦ, может стать вероятность безотказного обслуживания заявок на предоставление данных пользователям. Обозначим этот показатель  $W(t)$ , тогда для  $m$ -ого компонента (ветви) СХД

$$W_m(t) = R_m(1 - P_m), \quad (1)$$

где  $R_m$  – вероятность безотказной работы компонента (ветви) СХД;  $P_m$  – потери заявок на предоставление данных пользователям на компоненте (ветви) СХД;  $t$  – период времени безотказной работы каналов ветви, компонентов СХД.

Возможными типами отказов в СХД МДЦ могут быть занятость обслуживающих приборов, компонентов – каналов передачи данных, обеспечивающих ввод-вывод, хранение и транспортирование информации, а также серверов (блейд-серверов) дисков, дисковых массивов и библиотек СХД (качество) и выход из строя обслуживающего прибора (собственно надежность).

Причем для мобильных систем такого класса характерно применение именно блейд-серверов (так называемых, серверов-«лезвий») – ультракомпактных серверов, современных серверных массивов высокой плотности хранения (для уменьшения занимаемого пространства внутри МДЦ).

Тогда, с учетом всех компонентов (ветвей), входящих в состав СХД МДЦ, вероятность безотказного обслуживания заявок на предоставление данных пользователям определяется как

$$W_{ij}(t) = \prod_{r=1}^{k-1} W_{m_r}(t), \quad (2)$$

где  $m$  – компонент (ветвь) системы хранения,  $k$  – количество компонентов (ветвей),  $ij$  – путь от  $i$ -го компонента (ветви) до  $j$ -го компонента (ветви) СХД мобильного центра обработки данных.

Если между серверами, блейд-серверами, дисками, дисковыми массивами и библиотеками СХД МДЦ есть независимые пути – каналы передачи данных, обеспечивающие ввод-вывод, хранение и транспортирование информации, то вероятность безотказного обслуживания заявок на предоставление данных пользователям мобильных центров обработки данных определяется как

$$W_{ij}(t) = 1 - \prod_{g=1}^{X_{ij}} (1 - \prod_{r=1}^{k-1} W_{m_{rg}}(t)), \quad (3)$$

где  $X_{ij}$  – число независимых путей, связывающих блейд-серверы, диски, массивы и библиотеки СХД МДЦ [21, 23].

Вероятность безотказной работы  $m$ -ого компонента (ветви) СХД МДЦ, включающего в себя «узлы» данного компонента – блейд-серверы, диски, массивы данных и библиотеки, определяется в соответствии с выражением

$$R_m = \prod_{i=1}^{k-1} R_{mi}, \quad (4)$$

где  $R_{mi}$  – вероятность безотказной работы  $i$ -го «узла» – блейд-сервера, коммутатора, диска, массива данных или библиотеки в составе  $m$ -ого компонента (ветви) СХД МДЦ, которая определяется в соответствии с выражением

$$R_{mi} = K_{кр} e^{-\frac{t}{T_m}}, \quad (5)$$

где  $t$  – непрерывное время наработки на отказ,  $T_m$  – среднее время наработки на отказ,  $K_{кр}$  – коэффициент готовности, который определяется как

$$K_{кр} = \frac{T_m}{T_m + T_{mв}}, \quad (6)$$

где  $T_{mв}$  – среднее время восстановления.

Одним из традиционных методов анализа надежности сложных технических систем является логико-вероятностный метод (ЛВМ) оценки. При этом исходная постановка задачи и построение модели исследуемого объекта осуществляется структурными и аналитическими средствами математической логики, а расчет показателей надежности выполняется на основе методов теории вероятностей. Данный метод удобен для исходной формализованной постановки задач в виде структурного описания исследуемых свойств функционирования сложных технических систем [23].

В рамках ЛВМ задачу оценки надежности СХД МДЦ можно определить как задачу расчета показателей безотказности: вероятности безотказной работы за заданное время  $P(t)$ ; средней наработки на отказ  $T(T_1)$  и гамма-процентной наработки до отказа  $t_\gamma$ .

Расчет показателей безотказности СХД МДЦ основывается на структурной схеме надежности (СН) системы хранения и данных об интенсивностях отказов ее компонентов – каналов передачи данных, обеспечивающих ввод-вывод, хранение и транспортирование информации, а также блейд-серверов, дисков, дисковых массивов и библиотек (параметр потока отказов компонентов).

Показатели безотказности СХД МДЦ рассчитываются для интервала нормальной работы, когда наблюдается относительно постоянная интенсивность отказов компонентов

(элементов) системы хранения (параметр потока отказов восстанавливаемых компонентов), и допустимо использование для вычислений экспоненциального распределения случайного времени наступления таких отказов.

Структурная схема надежности СХД МДЦ для расчета показателей безотказности строится по следующим правилам: если отказ компонента (канала передачи данных, блейд-сервера, диска, дискового массива или библиотеки) приводит к отказу всей системы хранения (потеря хотя бы одной функции СХД), то этот компонент включается в ССН последовательно; если отказ компонента не приводит к отказу всей системы хранения (не теряется ни одна функция СХД), то такой элемент включается в ССН системы хранения МДЦ параллельно.

При последовательном соединении компонентов (каналов, блейд-серверов, дисков, дисковых массивов и библиотек) в структурной схеме надежности СХЖ МДЦ вероятность безотказной работы всей системы хранения равна произведению вероятностей безотказной работы компонентов:

$$P(t) = \prod_{i=1}^m P_i(t), \quad (7)$$

где  $m$  – компонент (ветвь) системы хранения.

При параллельном соединении элементов СХД МДЦ в структурной схеме надежности вероятность отказа всей системы хранения равна произведению вероятностей отказов компонентов:

$$Q(t) = \prod_{i=1}^m Q_i(t). \quad (8)$$

Основываясь на расчетных соотношениях (7) и (8), можно определить показатели безотказности СХД МДЦ. Так вероятность безотказной работы СХД на интервале нормальной работы можно выразить через экспоненциальное распределение [23]:

$$P(t) = e^{-\lambda t}, \quad (9)$$

где  $\lambda$  – интенсивность отказов компонентов (ветвей, элементов) системы хранения.

Учитывая выражение (7) для последовательного соединения компонентов (каналов, блейд-серверов, дисков, дисковых массивов и библиотек) в структурной схеме надежности СХД МДЦ и имея данные по интенсивностям отказов (параметр потока отказов восстанавливаемых компонентов СХД), вероятность безотказной работы системы хранения, например, из двух компонентов будет определяться выражением:

$$P(t) = P_1(t) \times P_2(t) = e^{-\lambda_1 t} \times e^{-\lambda_2 t} = e^{-(\lambda_1 + \lambda_2)t}. \quad (10)$$

В общем случае при последовательном соединении  $m$  компонентов (ветвей) СХД МДЦ вероятность безотказной работы системы хранения будет определяться выражением [21-23]:

$$P(t) = e^{-\left(\sum_i \lambda_i\right)t}. \quad (11)$$

Учитывая выражения (8) и

$$Q(t) = 1 - P(t), \quad (12)$$

для параллельного соединения компонентов (ветвей) в структурной схеме надежности СХД МДЦ, вероятность безотказной работы системы хранения, например, из двух компонентов (ветвей) будет определяться выражением:

$$P(t) = 1 - [1 - P_1(t)] \times [1 - P_2(t)] = 1 - [1 - e^{-\lambda_1 t}] \times [1 - e^{-\lambda_2 t}] = e^{-\lambda t}. \quad (13)$$

Этапы оценки параметров надежности СХД МДЦ, например, содержащей 6 (шесть) компонентов, взаимосвязанных в различные (параллельные, последовательные или гибридные) структуры, могут быть представлены в виде алгоритма, блок-схему которого иллюстрирует рисунок 1.

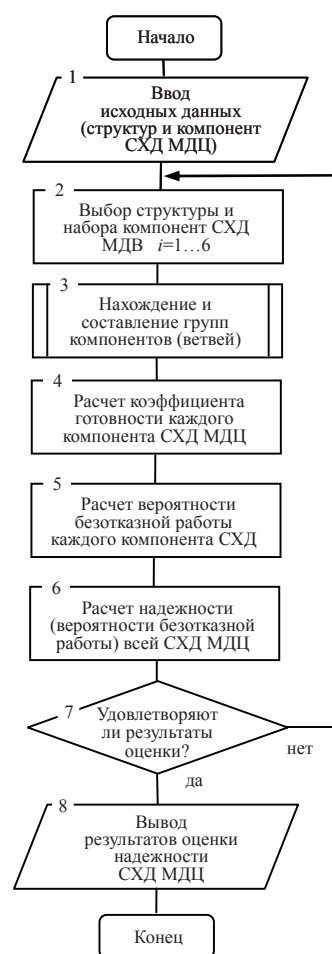


Рис. 1. Алгоритм оценки надежности СХД МДЦ

Таким образом, рассмотрены ключевые параметры надежности систем хранения и логико-вероятностный подход к их анализу, при помощи которого и с учетом математики теории надежности, могут быть реализованы этапы оценки параметров СХД МДЦ (см. рис. 1), опираясь на выражения (1)-(13), которые лягут в основу программного обеспечения по поддержке принятия решения в рамках выбора надежных систем хранения данных для МДЦ.

### Вариант реализации этапов оценки надежности систем хранения данных для мобильных дата-центров на основе программных средств

Для практической реализации этапов оценки параметров СХД МДЦ создано специальное программное обеспечение [24]. Программа написана на языке C++, среда разработки Visual Studio.

Рассмотрим особенности и возможности созданного программного средства для оценки надежности систем хранения данных мобильных дата-центров. Расчет параметров надежности осуществляется следующим образом.

Интерфейс программы при помощи манипулятора и скролла по правой стороне рабочего окна позволяет осуществить выбор необходимого варианта соединения компонентов (каналов, блейд-серверов, дисков, дисковых массивов и библиотек) СХД МДЦ. Выбранный тип, при наведении на него манипулятора, подсвечивается зеленым цветом. Выбор осуществляется нажатием левой клавиши манипулятора по варианту построения. После чего скроется главное окно и появится рабочее окно с выбранным типом (вариантом) построения и соединения компонентов СХД МДЦ (рис 2а). В рабочем окне находятся компоненты СХД МДЦ: каналы, коммутаторы, блейд-серверы, диски, дисковые массивы и библиотеки.

Под каждым компонентом размещен выпадающий список, позволяющий выбрать из имеющегося перечня компонентов (устройств) необходимые. В правом верхнем углу синим цветом подсвечивается цена всех указанных элементов. После выбора оборудования всех элементов необходимо нажать на кнопку «Рассчитать». На экране отобразится полная цена выбранного оборудования и вероятность безотказной работы всей системы хранения для данной схемы и набора компонент СХД МДЦ (рис. 2 б).

После ознакомления с итогами вычислений необходимо нажать на кнопку «ОК», закроется окно с результатом расчета надежности для данного варианта. Далее можно снова изменить исходные данные и рассчитать надежность той же или иной схемы СХД с другими компонентами – каналами, коммутаторами, блейд-серверами, дисками, дисковыми массивами.

Программное средство позволяет добавлять и удалять компоненты и устройства (каналы, коммутаторы, блейд-сервера, диски, дисковые массивы и библиотеки) из перечня, предоставленного в базе данных к данному приложению. Для этого необходимо воспользоваться функциями «Добавить устройства» либо «Удалить устройства», инициируется сервис (рабочее окно) для добавления и удаления компонентов СХД МДЦ, пример которого иллюстрирует рисунок 3.

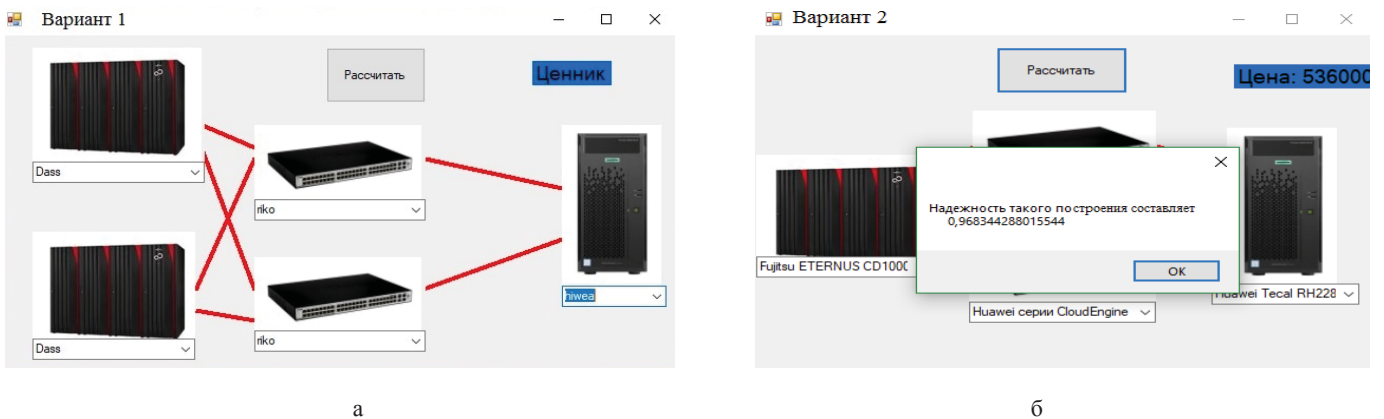


Рис. 2. Рабочее окно выбора и расчета программного средства «Оценка надежности СХД МДЦ»: а – на этапе выбора варианта схемы и компонент СХД МДЦ; б – на этапе получения оценки

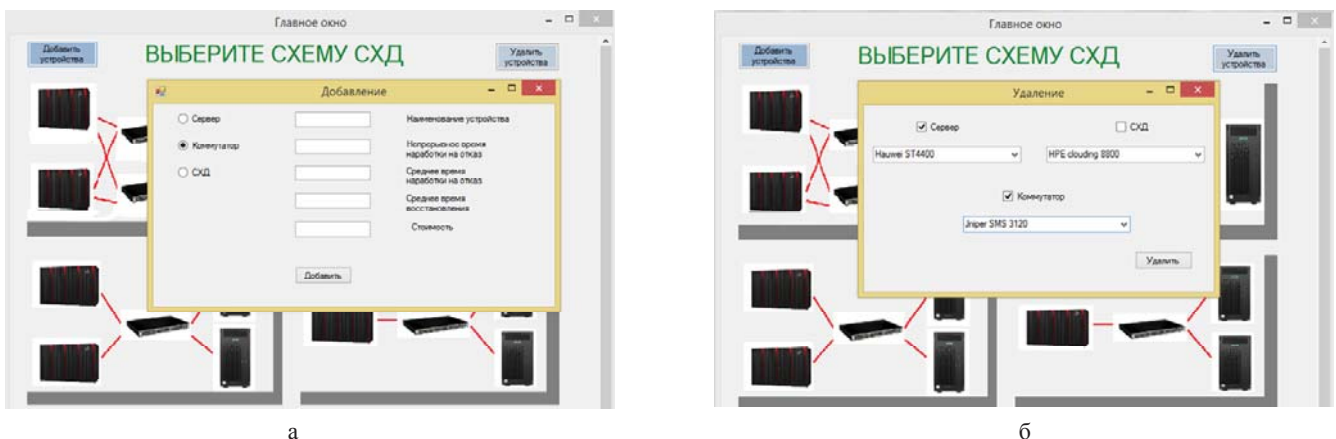


Рис. 3. Рабочее окно добавления и удаления компонент системы хранения в рамках программного средства «Оценка надежности СХД МДЦ»: а – на этапе добавления компонент СХД МДЦ в базу данных; б – на этапе удаления

Для добавления необходимо выбрать тип компонента (элемента, устройства) и заполнить, предоставляемые поля, инициировать функцию «Добавить», появится информационное окно, информирующее о том, что компонент (устройство) в базу данных программы добавлен.

Для того, чтобы новый, добавленный компонент (канал, коммутатор, блейд-сервер, диск, дисковый массив или библиотека) появился в выпадающих списках при оценке вариантов построения СХД, требуется перезапустить приложение.

Результаты вычислительного эксперимента – итоги расчета надежности вариантов СХД МДЦ приведены на рисунке 4.

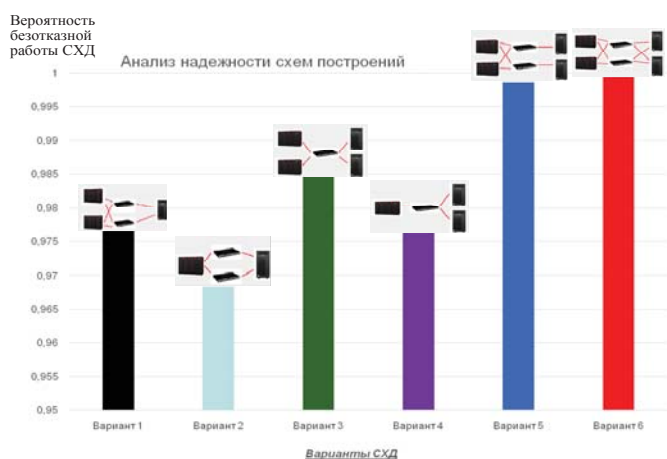


Рис. 4. Расчет надежности вариантов СХД МДЦ

Вычислительный эксперимент и результаты оценки надежности показывают, например, что из выбранного перечня компонентов (устройств) – систем хранения (дисков и дисковых массивов) надежнее оказался производитель марки Huawei. Его коэффициент надежности составляет 0,9986, что на 0,0006 превышает показания по надежности его оппонента Fujitsu. Программа позволяет осуществлять подобный анализ и для экономических показателей СХД МДЦ с точки зрения оценки суммарной стоимости выбранного варианта построения схемы системы хранения.

### Заключение

Таким образом, отсутствие современного метода оценки надежности систем хранения данных обуславливает актуальность и подчеркивает необходимость создания такого метода анализа. Проведен анализ систем хранения данных, рассмотрены и проанализированы существующие архитектуры систем хранения данных для МДЦ. Проанализированы и описаны преимущества и недостатки каждой архитектуры. Сделан предварительный вывод о потенциально более надежном типе СХД – SAN. Он представляет собой специализированную сеть хранения данных, которая функционирует параллельно с остальными элементами МДЦ и сети МДЦ, что и обуславливает его более надежную работу по сравнению с другими видами систем хранения.

Рассмотрены и описаны основные параметры, влияющие на оценку работы СХД МДЦ, а именно:  $K_{ГТ}$  – коэффициент

готовности,  $t$  – непрерывное время наработки на отказ,  $T_m$  – среднее время наработки на отказ,  $T_{mв}$  – среднее время восстановления и, в конечном итоге, как интегральный показатель – вероятность безотказной работы системы хранения данных мобильного дата-центра.

Проведен анализ методов анализа надежности, рассмотрены этапы оценки надежности систем хранения данных для мобильных дата-центров. Результатом анализа и выбора является логико-вероятностный метод оценки надежности, как наиболее рациональный с точки зрения оперативности и вычислительной сложности. Помимо этого, данный метод, при практически равных параметрах точности, выдаваемых результатов, прост в программной реализации.

При помощи логико-вероятностного метода и математики теории надежности разработан алгоритм оценки надежности систем хранения данных МДЦ. Алгоритм реализован в виде программного средства для анализа надежности систем хранения данных.

Практическим результатом исследований является создание программного средства «Оценка надежности СХД МДЦ», которое может выступать эффективным инструментом для поддержки принятия решения при выборе систем хранения на этапах проектирования, принятия проекта, замены или обновления СХД для мобильных центров обработки данных.

### Литература

1. Жигадло В.Э., Ногин С.Б. Сервисы центров обработки данных для абонентов «умного города» // Материалы XXVII международной научно-практической конференции «World Science: Problems and Innovations». МЦНС «Наука и просвещение». Пенза: 2018. С. 66-68.
2. Dutt D.G. Cloud Native Data Center Networking: Architecture, Protocols, and Tools. Sebastopol: O'Reilly Media, 2019. 486 p.
3. Ayomaya B.A. Data Center for Beginners: A beginner's guide towards understanding Data Center Design (Data Center Design Guide). New York: Computers & Technology Education, 2017. 62 p.
4. Докучаев В.А., Кальфа А.А., Маклачкова В.В. Архитектура центров обработки данных / Под ред. профессора В. А. Докучаева. М.: Горячая линия-Телеком, 2020. 240 с.
5. Brown M., Cartwright H., Gavanda M., Mauro A., Novak R., Valsecchi P. The Complete VMware vSphere Guide: Design a Virtualized Data Center with VMware vSphere 6.7. Birmingham: Packt Publishing, 2019. 768 p.
6. Carapola A. The Data Center Builder's Bible - Book 1: Defining Your Data Center Requirements: Specifying, Designing, Building and Migrating to New Data Centers. New York: NewVista Advisors, 2018. 227 p.
7. Михайличенко Н.В. Сравнительный анализ технологий построения региональных центров обработки данных // Юбилейная XV-ая Санкт-Петербургская международная конференция «Региональная информатика 2016». СПб.: СПОИСУ, 2016. С. 102-103.
8. Parker P.M. The 2021-2026 World Outlook for IT and Telecom Micro-Mobile Data Centers. New York: ICON Group International, Inc. 2020. 301 p.
9. De D. Mobile Cloud Computing: Architectures, Algorithms and Applications. Boca Raton: CRC Press Publishing, 2016. 377 p.
10. Huang D., Wu H. Mobile Cloud Computing: Foundations and Service Models. San Francisco: Morgan Kaufmann, 2017. 336 p.





11. *Авраменко В.С., Беденков В.Н., Селяков М.Н.* Прогнозирование защищенности информации в автоматизированных системах // Региональная информатика и информационная безопасность. СПб.: СПИОСУ, 2017. С. 26-27.
12. *Ткаченко В.В., Паращук И.Б., Зияев П.В.* Анализ тенденций применения и вопросы обеспечения информационной безопасности систем хранения данных для облачных технологий // Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России 2017». СПб.: СПОИСУ, 2017. С.88-89.
13. Мобильный модульный центр обработки данных. [Электронный ресурс] // ПитерЭнергоМаш. URL: <http://piterenergomash.ru/index.php/katalog-produksii/kontejnnye-resheniya/kontejnnye-tsod> (дата обращения 12.06.2021).
14. Мобильные центры обработки данных. [Электронный ресурс] // Инженерно-техническая компания «ИЛТОР». URL: <https://iltor.ru/projects/data-centry/> (дата обращения 12.06.2021).
15. *Новиков В.А.* Мобильный ЦОД GreenMDC TelecomOutdoor NGm – новый, компактный и масштабируемый // ЦОДы РФ. Проектирование, строительство, эксплуатация. 2017, № 20. С. 14–19.
16. *Темкин И.О., Баранникова И.В., Конов И.С.* Аппаратные средства хранения и обработки данных. М.: НИТУ «МИСИС», 2018. 44 с.
17. *Memon Q.A., Khoja S.A.* Data Science: Theory, Analysis and Applications. Boca Raton: CRC Press Publishing, 2019. 343 p.
18. *Arankalle C., Dwyer G., Geerdink B., Gera K., Liao K., Anand N.S.* The Artificial Intelligence Infrastructure Workshop: Build your own highly scalable and robust data storage systems that can support a variety of cutting-edge AI applications. Birmingham: Packt Publishing, 2020. 845 p.
19. *Strengholt P.* Data Management at Scale: Best Practices for Enterprise Architecture. Sebastopol: O'Reilly Media, 2020. 348 p.
20. *Deshpande P.S., Sharma S.C., Peddoju S.K.* Security and Data Storage Aspect in Cloud Computing (Studies in Big Data, 52) 1st ed. 2019 Edition. Springer. 2019. 97 p.
21. *Паращук И.Б., Саяркин Л.А., Ткаченко В.В.* К вопросу анализа качества и надежности комплексов средств защиты информации для современных систем хранения данных // Актуальные проблемы защиты и безопасности: Труды XX Всероссийской научно-практической конференции РАРАН. 3-4 апреля 2017. СПб.: ФГБУ «РАРАН», 2017. С. 250-253.
22. *Kotenko I.V., Parashchuk I.B.* Formation of Indicators for Assessing Technical Reliability of Information Security Systems // 2018 International Russian Automation Conference (RusAutoCon), 9-16 Sept. 2018, Sochi, Russia / IEEE Xplore Digital Library: Browse Conferences (2018). Vol. (Doc.) No.8501650. Pp. 1-6.
23. *Thomasian A.* Storage Systems: Organization, Performance, Coding, Reliability, and Their Data Processing. San Francisco: Morgan Kaufmann, 2021. 410 p.
24. *Ткаченко В.В., Паращук И.Б., Михайличенко Н.В., Зайцева А.А., Аржаева Д.А.* Свидетельство об официальной регистрации базы данных и программы для ЭВМ №18136 «Анализ надежности систем хранения данных центров обработки данных специального назначения». Регистрация от 24.05.2018. СПб.: ВАС. 2018. 28 с.

## QUESTIONS OF RELIABILITY ASSESSMENT OF MODERN DATA STORAGE SYSTEMS FOR MOBILE DATA CENTERS

**ELENA S. KRYUKOVA**

Saint-Petersburg, Russia, e.kkrukovaa69@yandex.ru

**VLADIMIR V. TKACHENKO**

Moscow, Russia, U-429@inbox.ru

**ANTON V. MIKHAILICHENKO**

Saint-Petersburg, Russia, katjuha777@inbox.ru

**IGOR B. PARASHCHUK**

Saint-Petersburg, Russia, shchuk@rambler.ru

**KEYWORDS:** *data storage system, mobile data center, reliability, component, assessment, method, algorithm, structure.*

### ABSTRACT

**Introduction:** the review is conducted in the field of modern approaches to the creation and improvement of methods for assessing the reliability of data storage systems of mobile data centers designed for the continuous provision of a high-quality set of basic and additional information services. At the same time, services are provided to consumers in any place of their location, where typical data centers solve not only the tasks of building the information infrastructure of organizations, departments and individual large enterprises, but also tasks focused on ensuring the information security of these infrastructures. The goals and objectives of data storage systems as the technological basis of mobile data centers, the features of architectures, technologies and conditions for their construction and operation are summarized and systematized. The reliability indicators of data storage systems are studied and formulated, the role and place of reliability assessment tasks are investigated. The relevance of ensuring the accuracy and multi-criteria reliability assessment in the interests of decision-making support for the design and construction of data storage systems is justified. The subject of the study is the reliability of data storage systems as a set of interconnected components (channels, switches, blade servers, disks, disk arrays, and libraries), as well as the con-

ditions for designing and building systems of this class that affect their reliability. **Purpose:** analysis of existing and development of new scientific and methodological tools and software for assessing the reliability of mobile data center data storage systems to ensure reliable and multi-criteria (taking into account the variety of components and interaction schemes) analysis of the reliability of both storage systems themselves and mobile data centers as a whole. **Results:** a method for analyzing the reliability of data storage systems for mobile data centers, consisting of a number of sequential steps, is proposed. The method and algorithm of its implementation are based on the logical-probabilistic approach to reliability assessment, are simple in software implementation and rational in terms of efficiency and computational complexity. **Practical relevance:** the presented approach allows us to formulate reliability indicators and evaluate the reliability of complex structures of data storage systems. A practical software implementation in C++ in the Visual Studio development environment has been implemented. The results of a computational experiment are obtained, which can serve as input data when making a decision on the choice of storage systems at the stages of design, project approval, replacement or update of data storage systems for mobile data centers.

### REFERENCES

1. Zhigadlo V.E., Nogin S.B. Servisy centrov obrabotki dannyh dlya abonentov "umnogo goroda" [Services of data processing centers for smart City subscribers] // Materials of the XXVII International scientific and practical conference "World Science: Problems and Innovations". ICNS "Science and Education". Penza: 2018. Pp. 66-68. (In Russian)
2. Dutt D.G. Cloud Native Data Center Networking: Architecture, Protocols, and Tools. Sebastopol: O'Reilly Media, 2019. 486 p.
3. Ayomaya B,A, Data Center for Beginners: A beginner's guide towards understanding Data Center Design (Data Center Design Guide). New York: Computers & Technology Education, 2017. 62 p.
4. Dokuchaev V.A., Kalfa A.A., Maklachkova V.V. Arhitektura centrov obrabotki dannyh [Architecture of data processing centers] / Ed. by Professor V.A. Dokuchaev. Moscow: Hotline-Telecom. 2020. 240 p. (In Russian)
5. Brown M., Cartwright H., Gavanda M., Mauro A., Novak R., Valsecchi P. The Complete VMware vSphere Guide: Design a Virtualized Data Center with VMware vSphere 6.7. Birmingham: Packt Publishing, 2019. 768 p.
6. Carapola A. The Data Center Builder's Bible - Book 1: Defining Your Data Center Requirements: Specifying, Designing, Building and Migrating to New Data Centers. New York: NewVista Advisors, 2018. 227 p.
7. Mikhailichenko N.V. Sravnitel'nyj analiz tekhnologij postroeniya regional'nyh centrov obrabotki dannyh



[Comparative analysis of technologies for building regional data centers] // The XV-th St. Petersburg international conference "Regional Informatics 2016". St. Petersburg: SPOISU, 2016. Pp. 102-103. (In Russian)

8. Parker P.M. The 2021-2026 World Outlook for IT and Telecom Micro-Mobile Data Centers. New York: ICON Group International, Inc. 2020. 301 p.

9. De D. Mobile Cloud Computing: Architectures, Algorithms and Applications. Boca Raton: CRC Press Publishing, 2016. 377 p.

10. Huang D., Wu H. Mobile Cloud Computing: Foundations and Service Models. San Francisco: Morgan Kaufmann, 2017. 336 p.

11. Avramenko V.S., Bedenkov V.N., Selyakov M.N. Forecasting of protection of information in automated systems // Regional'naya informatika i informacionnaya bezopasnost' [Regional science and information security]. St. Petersburg: SPOISU, 2017. Pp. 26-27. (In Russian)

12. Tkachenko V.V., Parashchuk I.B., Ziyayev P.V. Analiz tendencij primeneniya i voprosy obespecheniya informacionnoj bezopasnosti sistem hraneniya dannyh dlya oblachnyh tekhnologij [Analysis of application trends and issues of ensuring information security of data storage systems for cloud technologies] // St. Petersburg Interregional Conference "Information Security of Russian Regions 2017". St. Petersburg: SPOISU, 2017. Pp. 88-89. (In Russian)

13. Mobile modular data center. PeterEnergomash. URL: <http://piterenergomash.ru/index.php/katalog-produktsii/kontejnerye-resheniya/kontejnerye-tsod> (date of access 12.06.2021). (In Russian)

14. Mobile data centers. Engineering and technical company "ILTOR". URL: <https://iltor.ru/projects/data-center/> (date of access 12.06.2021). (In Russian)

15. Novikov V.A. MCOD GreenMDC TelecomOutdoor NGm - new, compact and scalable // Data Centers of the Russian Federation. Design, construction, operation. 2017, No. 20. Pp. 14-19. (In Russian)

16. Temkin I.O., Barannikova I.V., Konov I.S. Apparatsnye sredstva hraneniya i obrabotki dannyh [Hardware storage and

data processing]. Moscow: NUST MISIS, 2018. 44 p.

17. Memon Q.A., Khoja S.A. Data Science: Theory, Analysis and Applications. Boca Raton: CRC Press Publishing, 2019. 343 p.

18. Arankalle C., Dwyer G., Geerdink B., Gera K., Liao K., Anand N.S. The Artificial Intelligence Infrastructure Workshop: Build your own highly scalable and robust data storage systems that can support a variety of cutting-edge AI applications. Birmingham: Packt Publishing, 2020. 845 p.

19. Strengholt P. Data Management at Scale: Best Practices for Enterprise Architecture. Sebastopol: O'Reilly Media, 2020. 348 p.

20. Deshpande P.S., Sharma S.C., Peddoju S.K. Security and Data Storage Aspect in Cloud Computing (Studies in Big Data, 52) 1st ed. 2019 Edition. Springer. 2019. 97 p.

21. Parashchuk I.B., Sayarkin L.A., Tkachenko V.V. K voprosu analiza kachestva i nadezhnosti kompleksov sredstv zashchiteli informatsii dlya sovremennykh sistem sredeniya dannykh [On the issue of analyzing the quality and reliability of information security complexes for modern data storage systems]. Aktual'nye problemy zashchita i bezopasnosti: Trudy XX Vserossiyskoy nauchno-prakticheskoy konferentsii RARAN. 3-4 April 2017. St. Petersburg: FSBI "RARAN", 2017. Pp. 250-253. (In Russian)

22. Kotenko I.V., Parashchuk I.B. Formation of Indicators for Assessing Technical Reliability of Information Security Systems // 2018 International Russian Automation Conference (RusAutoCon), 9-16 Sept. 2018, Sochi, Russia / IEEE Xplore Digital Library: Browse Conferences (2018). Vol. (Doc.) No.8501650. Pp. 1-6.

23. Thomasian A. Storage Systems: Organization, Performance, Coding, Reliability, and Their Data Processing. San Francisco: Morgan Kaufmann, 2021. 410 p.

24. Tkachenko V.V., Parashchuk I.B., Mikhailichenko N.V., Zaitseva A.A., Arzhaeva D.A. Certificate of official registration of the database and computer program No.18136 "Analysis of the reliability of data storage systems of special-purpose data processing centers". Registration from 24.05.2018. St. Petersburg: VAS. 2018. 28 p. (In Russian)

#### INFORMATION ABOUT AUTHORS:

**Elena S. Kryukova** - Postgraduate student of the Military Telecommunication Academy, Saint-Petersburg, Russia

**Vladimir V. Tkachenko** - Senior Engineer, Moscow, Russia

**Anton V. Mikhailichenko** - Postgraduate student of the Military Telecommunication Academy, Saint-Petersburg, Russia

**Igor B. Parashchuk** - Full Professor, Doc. Nat. Sci., Ph.D. (in Technics), Professor of the Military Telecommunication Academy, Saint-Petersburg, Russia

doi: 10.36724/2409-5419-2021-13-5-96-102

# МЕТОДИКА ОБНАРУЖЕНИЯ АТАК, ТИПА SQL-ИНЪЕКЦИЯ НА ОСНОВЕ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, МЕТОДОМ ЗАДАЧИ КЛАССИФИКАЦИИ

**МИТРОФАНОВ**

Михаил Валерьевич<sup>1</sup>

**КРИБЕЛЬ**

Александр Михайлович<sup>2</sup>

**ФРОЛЕНКОВ**

Алексей Сергеевич<sup>3</sup>

**СПИЦЫН**

Олег Леонтьевич<sup>4</sup>

## АННОТАЦИЯ

**Введение:** компьютеризация системы жизнедеятельности современного общества с каждым днем набирает все более масштабные границы. В связи с этим, повышается и риск утраты и воровства конфиденциальной информации различными способами, в том числе и с помощью различных атак. **Цель исследования:** целью исследования является разработка оптимального метода обнаружения атак, на примере атак типа SQL-Injection, на основе заданного алгоритма работы искусственного интеллекта. **Методы:** предложена система обучения искусственного интеллекта на основе заданного алгоритма работы искусственного интеллекта. **Результаты:** в результате проведенной работы была предложена система обучения искусственных нейронных сетей для осуществления обнаружения признаков компьютерных атак на основе языка программирования SQL-Injection на информационно-коммуникационные системы в реальном времени на основе метода логической регрессии. Данную реализацию обнаружения атак типа SQL-Injection можно внедрить в серверную часть базы данных любого уровня, так как для защиты от данного типа атак необходимо тщательно фильтровать входные параметры, значения которых будут использованы для построения SQL-запроса и в случае обнаружения атаки заблокировать или перенаправить все запросы на заранее подготовленную фальшивую базу данных, что позволит повысить вероятность обнаружения компьютерных атак. **Практическая значимость:** на основе анализа сценариев нарушителя с привилегиями пользователя на локальном узле рассматривается одна из возможных реализаций обнаружения компьютерных атак вида SQL-инъекция методом логической регрессии. Для этого сгенерированы тренировочные данные и обнаружена атака обученной моделью. **Обсуждение:** реализация данной программы позволит осуществлять адаптивную защиту путем анализа поступивших запросов на сервер.

## Сведения об авторах:

<sup>1</sup> к.т.н., доцент, начальник кафедры Военная академия связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, mitrofanov223@mail.ru

<sup>2</sup> адъюнкт Военная академия связи им. Маршала Советского Союза С.М. Буденного, Россия, kribelllle@mail.ru

<sup>3</sup> курсант филиала Военного Учебного Научного центра Военно-воздушных Сил "Военно-воздушная Академия" имени профессора Н.Е. Жуковского и Ю.А. Гагарина в г. Челябинске, г. Челябинск, Россия, alexej.frolenkov@yandex.ru

<sup>4</sup> к.в.н., старший преподаватель Военная академия связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, idgarv@mail.ru

**КЛЮЧЕВЫЕ СЛОВА:** искусственная нейронная сеть, SQL-Инъекция, система защиты, информационная безопасность, информационно-телекоммуникационная сеть.

**Для цитирования:** Митрофанов М.В., Крибель А.М., Фроленков А.С., Спицын О.Л. Методика обнаружения атак, типа SQL-инъекция на основе алгоритмов искусственного интеллекта, методом задачи классификации // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 5. С. 96-102. doi: 10.36724/2409-5419-2021-13-5-96-102



## Введение

Мы живем в веке информационных технологий и нам приходится иметь дело с огромным массивом информации. Ежегодно генерируется 2,5 квинтиллиона байт данных. Человечество не способно воспользоваться подавляющей частью этой информации. Данные лежат за пределами возможностей стандартных аналитических методов, не говоря уже о нарастающем числе компьютерных атак, зачастую остающихся незамеченными. На рисунке 1, компанией Positive Technologies, представлен график классификаций жертв за 2019 год.

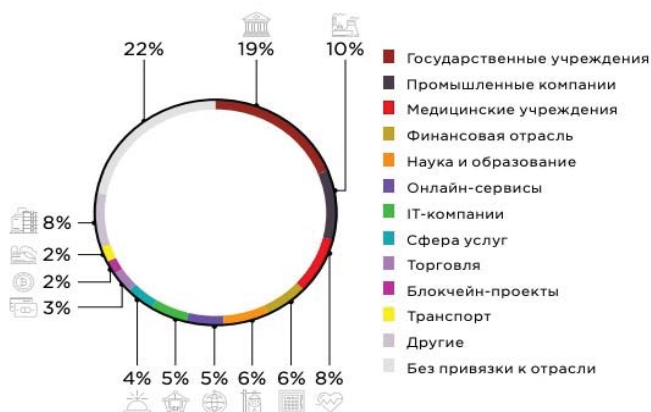


Рис. 1. Статистика жертв по отраслям

## Основная часть

С развитием компьютерных систем, которые человек использует в своей деятельности, все чаще и чаще появляются как новые языки программирования, так и развиваются способы, с помощью которых злоумышленники, на которых используются данные языки, получают доступ различными методами.

Основным языком программирования веб-сайтов, которые используют базы данных, является SQL, а метод, с помощью которого осуществляется атака на базы данных – является SQL-инъекция (SQL-Injection). Основная форма атаки SQL-инъекция состоит в прямой вставке кода в пользовательские входные переменные, которые объединяются с командами SQL и выполняются. Менее явная атака внедряет небезопасный код в строки, предназначенные для хранения в таблице или в виде метаданных.

SQL-Injection – метод, предназначенный для введения SQL запросов/команд через web-страницы. Многие web-страницы используют параметры, представленные пользователям сети интернет, и делают SQL запрос базы данных.

Для примера рассмотрим случай с логином пользователя, когда имеется web-страница с именем и паролем и производится SQL запрос в базе данных, для осуществления проверки, имеется ли зарегистрированный пользователь с таким именем и паролем. С использованием SQL-Injection можно послать придуманное имя пользователя и/или поле пароля, изменяющее SQL запрос, что может предоставить нам кое-что интересное.

Внедрение SQL-кода или SQL-инъекции – один из распространенных способов взлома сайтов и программ, рабо-

тающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода. Внедрение SQL, в зависимости от типа используемой системы управления базой данных (СУБД) и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.

Рассмотрим несколько типов атак на основе кода SQL-Injection:

- Классическая SQL Injection – простая и легкая в эксплуатации. Позволяет злоумышленнику атаковать БД и сразу видеть результат атаки. В последнее время встречается нечасто.

- Error-based SQL Injection – чуть более сложный и затратный по времени тип атаки, позволяющий, на основе выводимых ошибок СУБД, получить информацию о всей БД и хранящиеся в ней данные. Эксплуатируется, если кто-то в спешке забыл отключить вывод ошибок.

- Boolean-based SQL Injection – одна из «слепых» инъекций. Суть атаки сводится к добавлению специального подзапроса в уязвимый параметр, на который БД будет отвечать либо True, либо, неожиданно, False. Атака не позволяет сразу вывести все данные БД «на экран» злоумышленнику, но позволяет, перебирая параметры раз за разом, получить содержимое БД, хотя для этого потребуются временной отрезок соизмеримый с содержимым БД.

- Time-based SQL Injection – следующая из «слепых» инъекций. В данном случае злоумышленник добавляет подзапрос, приводящий к замедлению или паузе работы БД при некоторых условиях. Таким образом, атакующий, сравнивая время ответа на «True» и на «False» запросы, символ за символом может получить все содержимое БД, но времени уйдет на это больше, чем в случае эксплуатации Boolean-based атаки.

- Out-of-band SQL Injection – редкий тип. Атака может быть успешна только при определенных обстоятельствах, например, если сервер БД может генерировать DNS- или HTTP-запросы, что встречается нечасто. Также, как и Blind SQL, позволяет посимвольно собирать информацию о хранящихся там данных.

Рассмотрим возможные типы SQL инъекции на базы данных пользователей, которые возможны, основываясь на рассмотренных типах атаки на основе кода SQL-Injection:

- 1) Наиболее простые – сворачивание условия WHERE к истинностному результату при любых значениях параметров.

- 2) Присоединение к запросу результатов другого запроса. Делается это через оператор UNION.

- 3) Закомментирование части запроса.

Когда впоследствии сохраненные строки объединяются с динамической командой SQL, происходит выполнение небезопасного кода. Атака осуществляется посредством преждевременного завершения текстовой строки и присоединения к ней новой команды. Поскольку к вставленной команде перед выполнением могут быть добавлены дополнительные строки, злоумышленник заканчивает внедряемую строку меткой комментария «--». Весь последующий текст во время выполнения не учитывается.

Суть уязвимости – выполнение произвольного запроса к базе данных. Запрос может быть любым: на чтение, запись, модификацию и удаление каких-либо записей. Чтобы сделать базу данных более безопасной, ее можно разделить на несколько частей. В области информационной безопасности существует такое понятие, как принцип минимальных привилегий. Суть принципа состоит в том, что программа или пользователь должны иметь доступ только к тому, что им нужно и нечему больше. А ведь этими угрозами все не ограничивается, так как при определенных обстоятельствах можно добраться и до чтения/записи локальных файлов или даже до выполнения кода! Все зависит от целей, которые преследует злоумышленник, от используемой системы и того, как она сконфигурирована.

Несмотря на то, что государственные, финансовые, медицинские учреждения и промышленные компании в большей степени страдают от хакерских атак, им подвергаются абсолютно все отрасли нашей жизни.

На рисунке 2, компанией Positive Technologies, представлен обзор тактик и техник таргетированных атак на государственные сектора в России за 2019 год.

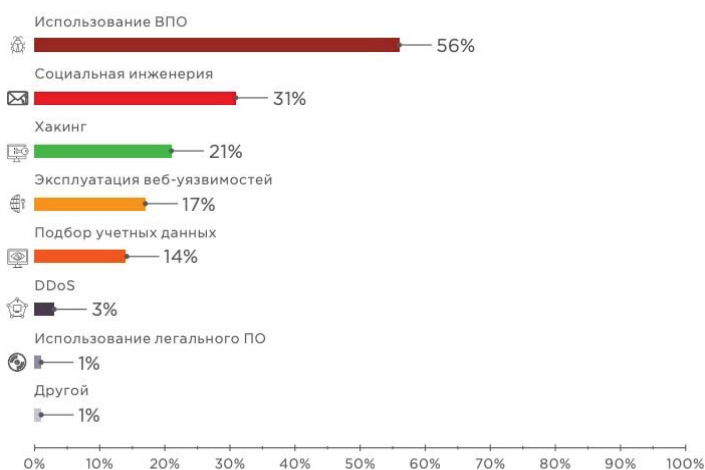


Рис. 2. АРТ-атаки на госучреждения в России

Как видно из рисунка 2, к преобладающему числу методов проникновения относят использование вредоносного программного обеспечения, социальную инженерию, хакинг, эксплуатацию web-уязвимостей а также подбор учетных данных.

В качестве примера проникновения с использованием данных методов, можно привести несколько сценариев нарушителя (рис. 3 и 4).

Как правило, сценарий «нарушителя с привилегиями пользователя на локальном узле» вытекает из сценария «внешнего нарушителя» и несет за собой полный контроль над системой злоумышленником.

В случае если взломом занимается группа профессионалов, оба сценария кибератак сложно выявить традиционными сигнатурными методами, тем самым довольно редко можно избежать разрушительных последствий и чудовищных убытков на стороне атакуемого.

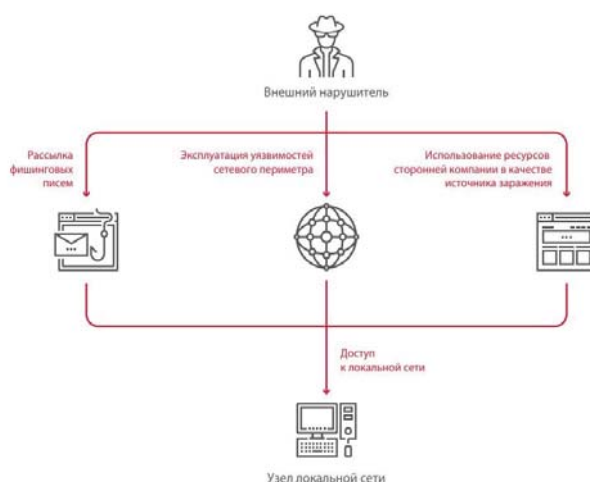


Рис. 3. Сценарий нарушителя

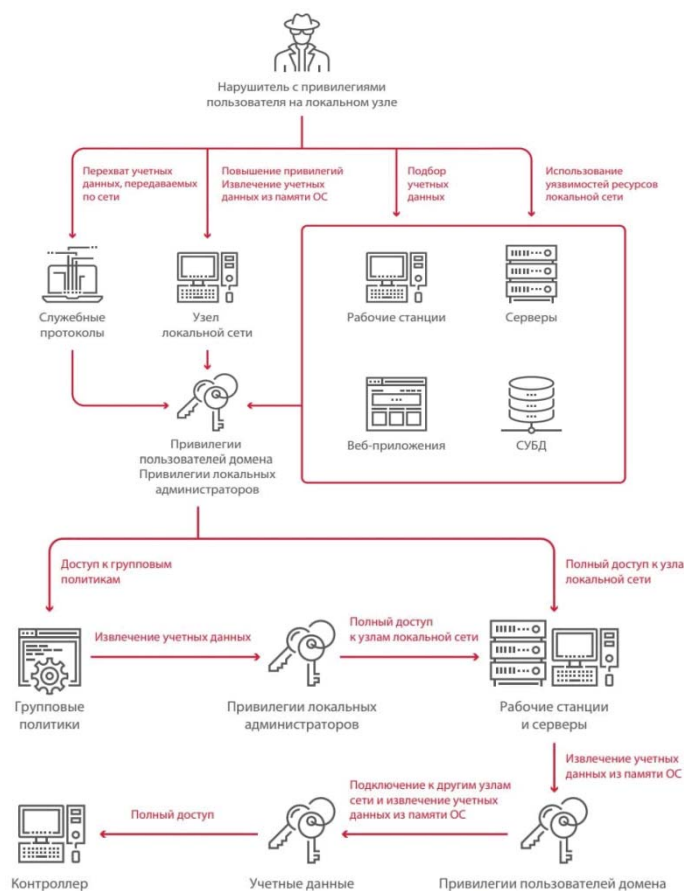


Рис. 4. Сценарий нарушителя с привилегиями пользователя на локальном узле

В настоящее время существуют перспективные методы, благодаря которым можно обучить компьютеры обрабатывать большие объемы данных и находить скрытые угрозы в информационной безопасности.

В 1943 г. Уоррен Маккалок и Уолтер Питтс опубликовали концепцию упрощенной клетки головного мозга (рис. 5).

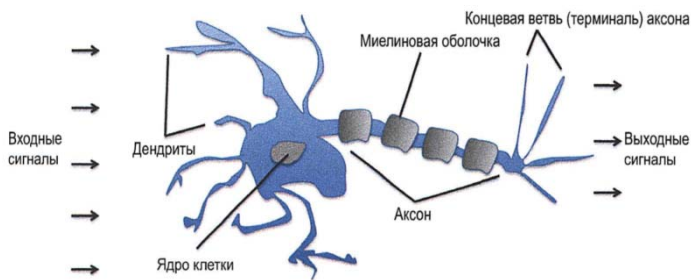


Рис. 5. Упрощенная схема нейрона

Питтс и Маккалок описали такую клетку в виде простого логического элемента с бинарными входами и назвали ее нейронным перцептроном. Как проиллюстрировано на рисунке 5, входные сигналы поступают в дендриты, затем интегрируются в клеточное тело, и если накопленный сигнал превышает порог, то генерируется выходной сигнал, который аксоном передается к следующей клетке.

В работе «Перцептрон, воспринимающий и распознающий автомат» 1957 г. Фрэнк Розенблатт представил правила обучения перцептрона и предложил алгоритм, который автоматически обучался оптимальным весовым коэффициентам, которые затем перемножались с входными признаками для принятия решения о том, активировать нейрон или нет.

Для обучения искусственного интеллекта, как правило, используют три вида обучения: обучение с учителем, обучение без учителя и обучение с подкреплением. Каждый вид должен обладать способностью к обобщению эмпирических фактов, иными словами уметь восстановить зависимость между ситуациями и реакциями, выдавая при этом достаточно точный ответ.

Модель, основанная на обучении с учителем, позволяет делать прогнозы о ранее не встречавшихся данных. Выборки, используемые для обучения такого алгоритма, должны содержать в себе не только набор примеров, но и правильных ответов с экспертной точки зрения. Под «учителем» понимается либо эксперт, который указал на заданных объектах правильные ответы, либо сама выборка.

К прикладным задачам такого метода относятся: медицинская диагностика, предсказание месторождений полезных ископаемых, принятие инвестиционных решений на финансовом рынке.

Модель, основанная на обучении с подкреплением, обучается посредством взаимодействия со средой. Откликом среды на принятые решения, являются сигналы подкрепления [1, 9], поэтому такое обучение является частным случаем обучения с учителем, с разницей в том, что учителем является не эксперт, а модель или среда.

Впервые, обучение с обратной связью, было предложено М.Л. Цетлином в 1961 г. Он поместил конечный автомат во внешнюю среду, которая с вероятностями, зависящими от совершаемого автоматом действия, наказывала или поощряла автомат. В соответствии с реакцией среды автомат самостоятельно изменял своё внутреннее состояние, что приводило к постепенному снижению числа наказаний, то есть обучению [2, 7].

Модель, основанная на обучении без учителя, обучается на спонтанных немаркированных данных без вмешательства

со стороны экспериментатора. Как правило, это актуально только для задач, в которых среди известных множеств объектов требуется обнаружить внутренние зависимости.

В анализе данных, алгоритмы, основанные на обучении с учителем, используют методы классификации и регрессии.

Суть задачи классификации заключается в идентификации категориальных меток классов для новых экземпляров на основе предыдущих наблюдений. Данный термин произошел из задачи машинного зрения, поэтому чаще употребляется синоним – распознавание образов или дискриминантный анализ. В классической задаче классификации обучающая выборка представлена виде  $X = \{x_i\}_{i=1}^n$ , где  $x_i$  – вектор вещественнозначных признаков  $x_i = (x_{i,1}, \dots, x_{i,d})$ . В качестве исхода объекта  $x$  фигурирует переменная  $t$ , принимающая конечное число значений, обычно из множества  $T = \{1, \dots, n\}$ . При классификации, каждая единица наблюдения относится к определенной группе на основе некоторого качественного свойства.

Метод классификации применим для поиска аномалий, однако существует проблема, связанная с выбором обучающих примеров. Аномалии – редкое явление и их примеров исчезающее мало. На практике такой задачей, является мошенничество с банковскими картами.

С помощью регрессионного анализа можно восстанавливать зависимость между переменными с предсказанием непрерывных результатов. Регрессия легко моделируется, но имеет недостаток, который заключается в чрезмерной зависимости от объема и сложности данных [3, 5].

В рамках обнаружения атаки типа SQL-Иньекция, в качестве метода построения линейного классификатора, позволяющего оценивать апостериорные вероятности принадлежности объектов классам, выбран частный случай обобщенной линейной регрессии – логистическая регрессия (рис. 6).

В отличие от обычной регрессии, в методе логистической регрессии не производится предсказание значения числовой переменной исходя из выборки исходных значений. Вместо этого, значением функции является вероятность того, что данное исходное значение принадлежит к определенному классу [4, 6, 8].

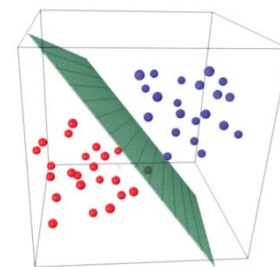


Рис. 6. Дискриминация точек на различные классы методом логистической регрессии

На рисунке 7 изображены данные необходимые для тренировки модели. Вторым столбцом являются заранее известные ответы, выступающие в роли учителя, контролирующего учебный процесс. Имея правильные ответы, алгоритм итеративно делает прогнозы на тренировочных данных и корректируется.



	A	B
1	214564	0
2	214564	0
3	1)) or sleep(__TIME__)#	1
4	kribel@mail.ru	0
5	email@mail.ru	0
6	\\'; DESC users; --	1
7	""info	0
8	email@mail.ru	0
9	fgfhghghgh	0
10	dsflkjdsfds	0
11	1\`1	1
12	dsflkjdsfds	0
13	dsflkjdsfds	0
14	kribel@mail.ru	0
15	email@mail.ru	0
16	" or sleep(__TIME__)#	1
17	1\` AND 1=(SELECT COUNT(*) FROM	1
18	1\` AND non_existant_table = \`1	1
19	1 AND USER_NAME() = \`dbo\`	1
20	1\\\`1	1
21	214564	0
22	1 AND 1=1	1
23	1 EXEC XP_	1
24	1\` OR \`1\`=\`1	1

Рис. 7. Сгенерированные тренировочные данные

На рисунке 8 изображен вывод результата обученной модели.

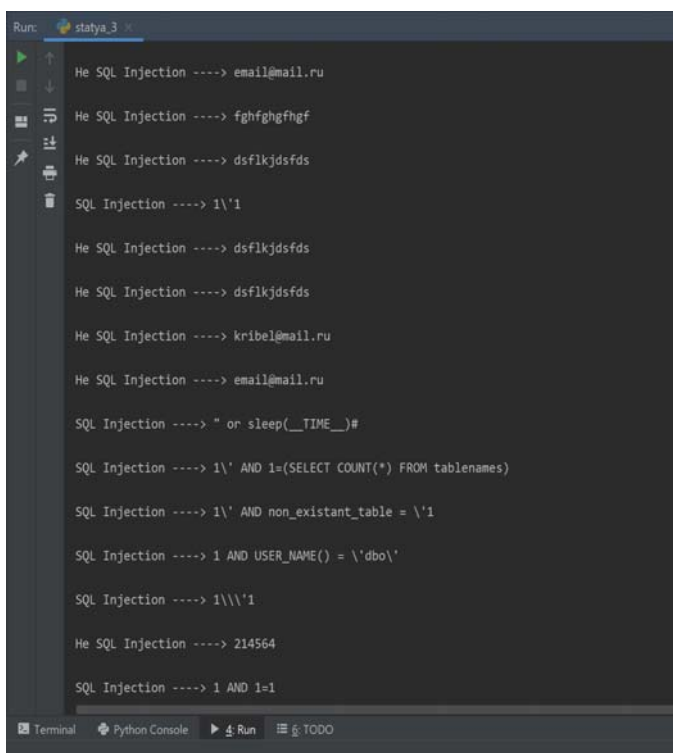


Рис. 8. Обнаружение атак

## Заключение

Таким образом, данную реализацию обнаружения SQL-Инъекция можно внедрить в серверную часть, и в случае обнаружения атаки блокировать или перенаправлять все запросы на фальшивую базу данных, что позволит повысить вероятность обнаружения компьютерных атак.

## Литература

1. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П., Муртазин И.Р. Методика прогнозирования воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // В сборнике: Региональная информатика и информационная безопасность. 2017. С. 109-111.
2. Гудков М.А., Лаута О.С., Иванов Д.А., Соловьев Д.В. Применение методов искусственного интеллекта в задачах обеспечения информационной безопасности // Современные информационные технологии. 2018. С. 162.
3. Коцыняк М.А., Карнов М.А., Лаута О.С., Дементьев В.Е. Управление системой обеспечения безопасности информационно-телекоммуникационной сетью на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. 2020. № 4. С. 3-10.
4. Л. Черняк <https://www.osp.ru/os/2018/03/13054415/> OSP – Гид по технологиям цифровой трансформации
5. Багрецов С.А., Лаута О.С., Михаил И.И., Михайлец А.Н., Бойко Д.А. Повышение устойчивости информационно-телекоммуникационной сети в условиях воздействия противника // I-methods. 2020. Т. 12. № 2. С. 1-13.
6. Данилова Е.И., Лаута О.С., Ракицкий Д.С., Ракицкий С.Н. Подход к построению модели целевых кибернетических воздействий // В сборнике: Актуальные проблемы защиты и безопасности Труды XXII Всероссийской научно-практической конференции РАРАН. 2019. С. 210-213.
7. Белякова Т.В., Лаута О.С., Хохлачева Е.А. Модель воздействия целевых компьютерных атак на киберфизическую систему // В сборнике: Радиолокация, навигация, связь Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А.С. Попова. В 6-ти томах. 2019. С. 320-324.
8. Архитектура сети подвижной радиосвязи на основе эталонной модели взаимодействия открытых систем // В сборнике: Радиолокация, навигация, связь Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А.С. Попова: в 6-ти томах. Воронежский государственный университет, АО "Концерн "Созвездие". 2019. С. 173-182.
9. Баранов В.В., Максимова Е.А., Лаута О.С. Анализ модели информационного обеспечения процессов и систем при реализации многоагентного интеллектуального взаимодействия // Приборы и системы. Управление, контроль, диагностика. 2019. № 4. С. 32-41.
10. Власенко М.А., Иванов Д.А., Кузнецов С.И., Лаута О.С. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция // Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 167-171.
11. Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П., Муртазин И.Р. Методика прогнозирования воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // В сборнике: Региональная информатика и информационная безопасность. 2017. С. 109-111.
12. Коцыняк М.А., Иванов Д.А. Обеспечение безопасности управления роботизированных систем от воздействия таргетированных кибернетических атак В книге: Нейрокомпьютеры и их применение. Тезисы докладов. 2018. С. 108-А.
13. Коцыняк М.А., Лаута О.С., Иванов Д.А., Лукина О.М. Модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 3-4 (129-130). С. 58-65.



14. Лаута О.С., Иванов Д.А., Нечепуренко А.П., Власенко М.А. Методика синтеза системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства // В сборнике: Радиолокация, навигация, связь // Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 124-129.

15. Гудков М.А., Лаута О.С., Иванов Д.А., Соловьев Д.В. Применение методов искусственного интеллекта в задачах обеспечения информационной безопасности // Современные информационные технологии. 2018. С. 162.

16. Лаута О.С., Коцыняк М.А., Иванов Д.А., Суетин А.И. Методика прогнозирования воздействия компьютерных атак на информационно-телекоммуникационную сеть В сборнике: Радиолокация, навигация, связь // Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 115-123.

17. Иванов Д.А., Мамай А.В., Стицын О.Л., Карасев И.В. Подход к обоснованию структуры воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. № 2 (34). С. 107-110.

18. Коцыняк М.А., Лаута О.С., Иванов Д.А., Кузнецов С.И. Применение международного стандарта iso/iec 27032:2012, регламентирующего политическую и военную деятельность в киберпространстве // В сборнике: Современные информационные технологии. Теория и практика. Материалы IV Всероссийской научно-практической конференции. Отв. ред. Т.О. Петрова. 2018. С. 192-196.

19. Кузнецов С.И., Иванов Д.А., Власенко М.А., Латушко Н.А. Вероятностно-временные характеристики атак на роботизированные системы // В сборнике: Региональная информатика и информационная безопасность. 2017. С. 117-118.

20. Багрецов С.А., Лаута О.С., Щукин А.В., Иванов Д.А. Методика обоснования эффективной групповой деятельности операторов с двухуровневой структурой организации // Известия Тульского государственного университета. Технические науки. 2021. № 6. С. 20-29.

21. Багрецов С.А., Лаута О.С., Михаил И.И., Иванов Д.А. Методика обоснования рационального количества резервных каналов связи в информационно-телекоммуникационной сети // Электро-связь. 2020. № 8. С. 31-38.

## THE METHOD OF DETECTING ATTACKS, SUCH AS SQL-INJECTION BASED ON ARTIFICIAL INTELLIGENCE ALGORITHMS, BY THE METHOD OF THE CLASSIFICATION PROBLEM

**MIKHAIL V. MITROFANOV**

St-Petersburg, Russia, mitrofanov223@mail.ru

**ALEXANDER M. KRIBEL**

St-Petersburg, Russia, kribellllle@mail.ru

**ALEXEY S. FROLENKOV**

Chelyabinsk, Russia, alexej.frolenkov@yandex.ru

**OLEG L. SPITSYN**

St-Petersburg, Russia, idgarv@mail.ru

**KEYWORDS:** artificial neural network, SQL-Injection, security system, information security, information and telecommunications network.

### ABSTRACT

**Introduction:** computerization of the vital activity system of modern society is gaining more and more large-scale boundaries every day. In this regard, the risk of loss and theft of confidential information in various ways, including through various attacks, also increases. **Purpose:** the aim of the study is to develop an optimal method for detecting attacks, using the example of SQL-Injection attacks, based on a given algorithm of artificial intelligence. **Methods:** a training system for artificial intelligence based on a given algorithm of artificial intelligence is proposed Results: as a result of the work carried out, a training system for artificial neural networks was proposed to detect signs of computer attacks based on the SQL-Injection programming language on information and communication systems in real time based on the

logical regression method. This implementation of detecting SQL-Injection attacks can be implemented in the server part of a database of any level, since to protect against this type of attacks, it is necessary to carefully filter the input parameters whose values will be used to build an SQL query and, if an attack is detected, block or redirect all requests to a pre-prepared fake database, which will increase the probability of detecting computer attacks. Practical relevance: based on the analysis of scenarios of an intruder with user privileges on a local node, one of the possible implementations of detecting computer attacks of the type SQL injection by the method of logistic regression is considered. To do this, training data is generated and an attack is detected by a trained model. **Discussion:** the implementation of this program will allow for adaptive protection by analyzing received requests to the server.

## REFERENCES

1. Kotsynyak M. A., Ivanov D. A., Lauta O. S., Nechepurenko A. P., Murtazin I. R. (2017). Methodology for predicting the impact of a targeted cyber attack on an information and telecommunications network. *In the collection: Regional Informatics and information security*. Pp. 109-111. (In Russian)
2. Gudkov M. A., Lauta O. S., Ivanov D. A., Solovyov D. V. (2018). Application of artificial intelligence methods in information security problems. *Modern information technologies*. P. 162. (In Russian)
3. Kotsynyak M. A., Karpov M. A., Lauta O. S., Dementyev V. E. (2020). Management of the information and telecommunications network security system based on algorithms for the functioning of an artificial neural network". *Proceedings of the Tula State University. Technical sciences*. No. 4. pp. 3-10. (In Russian)
4. L. Chernyak <https://www.osp.ru/os/2018/03/13054415> / OSP-Guide to Digital Transformation Technologies.
5. Bagretsov S. A., Lauta O. S., Mikhail I. I., Mikhailets A. N., Boyko D. A. (2020). Increasing the stability of the information and telecommunications network under the influence of the enemy. *I-methods*. Vol. 12. No. 2. pp. 1-13. (In Russian)
6. Danilova E. I., Lauta O. S., Rakitsky D. S., Rakitsky S. N. (2019). Approach to building a model of targeted cybernetic influences. *In the collection: Actual problems of protection and security Proceedings of the XXII All-Russian Scientific and Practical Conference RARAN*. Pp. 210-213. (In Russian)
7. Belyakova T. V., Lauta O. S., Khokhlacheva E. A. (2019). Model of the impact of targeted computer attacks on a cyber-physical system. *In the collection: Radar, navigation, communication Proceedings of the XXV International Scientific and Technical Conference dedicated to the 160th anniversary of the birth of A. S. Popov*. In 6 volumes. Pp. 320-324. (In Russian)
8. Mobile radio network architecture based on the reference model of open systems interaction. *In the collection: Radar, navigation, communication Proceedings of the XXV International Scientific and Technical Conference dedicated to the 160th anniversary of the birth of A. S. Popov*: in 6 volumes. Voronezh State University, JSC "Concern " Constellation". 2019. pp. 173-182. (In Russian)
9. Baranov V. V., Maksimova E. A., Lauta O. S. (2019). Analysis of the model of information support of processes and systems in the implementation of multi-agent intelligent interaction. *Devices and systems. Management, monitoring, diagnostics*. No. 4. pp. 32-41. (In Russian)
10. Vlasenko M. A., Ivanov D. A., Kuznetsov S. I., Lauta O. S. (2018). In the collection: Actual problems of infotelecommunications in science and education (APINO 2018). *VII International Scientific-technical and scientific-methodological Conference. Collection of scientific articles*. In 4 volumes. Edited by S. V. Bachevsky. Pp. 167-171. (In Russian)
11. Kotsynyak M. A., Ivanov D. A., Lauta O. S., Nechepurenko A. P., Murtazin I. R. (2017). Methodology for predicting the impact of a targeted cyber attack on an information and telecommunications network *In the collection: Regional Informatics and information security*. Pp. 109-111. (In Russian)
12. Kotsynyak M. A., Ivanov D. A. (2018). Ensuring the security of the control of robotic systems from the impact of targeted cybernetic attacks. In the book: *Neurocomputers and their application*. Abstracts of reports. P. 108-A. (In Russian)
13. Kotsynyak M. A., Lauta O. S., Ivanov D. A., Lukina O. M. (2019). Model of the impact of a targeted cyber attack on the information and telecommunications network *Issues of defense technology. Series 16: Technical means of countering terrorism*. No. 3-4 (129-130). pp. 58-65. (In Russian)
14. Lauta O. S., Ivanov D. A., Nechepurenko A. P., Vlasenko M. A. (2018). Method of synthesis of the information and telecommunications network protection system in the conditions of information confrontation. *In the collection: Radar, navigation, communication. Proceedings of the XXIV International Scientific and Technical Conference*. In 5 volumes. Pp. 124-129. (In Russian)
15. Gudkov M. A., Lauta O. S., Ivanov D. A., Solovyov D. V. (2018). Application of artificial intelligence methods in information security problems. *Modern information technologies*. P. 162. (In Russian)
16. Lauta O. S., Kotsynyak M. A., Ivanov D. A., Suetin A. I. (2018). Methodology for predicting the impact of computer attacks on the information and telecommunications network *In the collection: Radar, navigation, communication. Proceedings of the XXIV International Scientific and Technical Conference*. In 5 volumes. Pp. 115-123. (In Russian)
17. Ivanov D. A., Mamai A.V., Spitsyn O. L., Karasev I. V. (2019). Approach to substantiating the structure of the impact of a targeted cybernetic attack on the information and telecommunications network. *Information technologies and systems: management, economics, transport, law*. No. 2 (34). pp. 107-110. (In Russian)
18. Kotsynyak M. A., Lauta O. S., Ivanov D. A., Kuznetsov S. I. (2018). Application of the international standard iso/iec 27032:2012 regulating political and military activities in cyberspace. *In the collection: Modern information technologies. Theory and practice. Materials of the IV All-Russian Scientific and Practical Conference*. Ed. by T. O. Petrov. Pp. 192-196. (In Russian)
19. Kuznetsov S. I., Ivanov D. A., Vlasenko M. A., Latushko N. A. (2017). Probabilistic-temporal characteristics of attacks on robotic systems. *In the collection: Regional informatics and information security*. Pp. 117-118. (In Russian)
20. Bagretsev S. A., Lauta O. S., Shchukin A.V., Ivanov D. A. (2021). Methodology for substantiating the effective group activity of operators with a two-level organization structure. *Izvestiya Tula State University. Technical sciences*. No. 6. pp. 20-29. (In Russian)
21. Bagretsov S. A., Lauta O. S., Mikhail I. I., Ivanov D. A. (2020). Methodology for substantiating the rational number of backup communication channels in the information and telecommunications network. *Telecommunications*. No. 8. pp. 31- (In Russian)

## INFORMATION ABOUT AUTHORS:

**Mikhail V. Mitrofanov** - PhD, Docent, Head of Department of the military Academy of Communications, St-Petersburg, Russia

**Alexander M. Kribel** - Postgraduate at the Department of the military Academy of Communications, St-Petersburg, Russia

**Alexey S. Frplenkov** - Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin in Chelyabinsk, Chelyabinsk, Russia

**Oleg L. Spitsyn** - PhD, Senior lecturer of the military Academy of Communications, St-Petersburg, Russia

**For citation:** Mitrofanov M.V., Kribel A.M., Frolenkov A.S., Spitsyn O.L. The method of detecting attacks, such as SQL-injection based on artificial intelligence algorithms, by the method of the classification problem. *H&ES Reserch*. 2021. Vol. 13. No. No 5. P. 96-102. doi: 10.36724/2409-5419-2021-13-5-96-102 (In Rus)