Научно-технический журнал

H&ES RESEARCH

Scientific and Technical Journal

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 технологий космических исследований Земли.

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

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

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

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.

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

JOURNAL H&ES RESEARCH INDEXING

• 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** и библиотеке **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.**
С требованиями можно ознакомиться на сайте: **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.

All issues of the journal are in a free access on a site of the journal **www.hes.ru** and **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.**
The requirements are available on the website: **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 Rur.
Postgraduate students for publication
of the manuscript will not be charged

T. 12
6
2020

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU Дата выхода: 25 декабря 2020

Учредитель:
ООО «ИД Медиа Паблишер»

Издатель:
ДЫМКОВА С.С.

Главный редактор:
ЛЕГКОВ К.Е.

Адрес издателя:
111024, Россия, Москва,
ул. Авиамоторная, д. 8, офис 512-514.

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.

СОДЕРЖАНИЕ

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

РАДИОТЕХНИКА И СВЯЗЬ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

CONTENTS

Founder:
"Media Publisher", LLC

Publisher:
DYMKOVA S.S.

Editor in chief:
LEGKOV K.E.

Address of publisher:
111024, Russia, Moscow,
st. Aviamotornaya, 8, office 512-514;

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

doi: 10.36724/2409-5419-2020-12-6-4-10

АЛГОРИТМ ТРАЕКТОРНОЙ ОБРАБОТКИ ИНФОРМАЦИИ РАДИОЛОКАЦИОННЫХ ИЗМЕРИТЕЛЬНЫХ КОМПЛЕКСОВ НА ОСНОВЕ КЛАСТЕРИЗАЦИИ МЕТОДОМ K-MEANS

КОНДЫБАЕВ
Нурлан Сакенович[1]

КУПРИЯНОВ
Николай Александрович[2]

КУРАКИН
Сергей Зосимович[3]

АННОТАЦИЯ

Рассматривается проблемная ситуация, обусловленная необходимостью повышения точности определения радиолокационными измерительными комплексами местоположения наблюдаемых космических объектов. Показано, что точностные характеристики радиолокационных измерительных комплексов зависят от величины вклада различных погрешностей измерений, наиболее значимыми из которых для современных высокоинформативных средств наблюдения являются атмосферные, определяемые гелиогеофизическими условиями функционирования. Отмечено, что применяемые в настоящее время подходы к компенсации атмосферных погрешностей измерений не позволяют учитывать гелиогеофизические условия функционирования радиолокационных измерительных комплексов с высоким временным и пространственным разрешением. Показано, что при обработке координатной информации не в полной мере учитываются спорадические изменения гелиогеофизических условий функционирования, что ведёт к росту ошибок измерений местоположения космических объектов и снижению информационных возможностей радиолокационных измерительных комплексов. Рассмотрена идея использования невязки измерений радиолокационным измерительным комплексом местоположения космических объектов, по которым имеется априорная координатная информация. Показаны результаты объединения методами кластерного анализа групп измерений местоположения космических объектов. Представлены результаты компьютерного моделирования и показано, что предложенный подход позволяет определять области, в которых влияние гелиогеофизических условий функционирования увеличивает погрешности измерений. Изложены основные расчётные соотношения и показаны этапы алгоритма траекторной обработки информации радиолокационных измерительных комплексов на основе кластеризации методом K-MEANS. Предложены дальнейшие направления использования результатов работы алгоритма, заключающиеся в использовании данных о сформированных кластерах для обработки информации о космических объектах, по которым отсутствует априорная координатная информация. Показано, что предложенный подход может быть применен в целях повышения информационных возможностей радиолокационных измерительных комплексов.

КЛЮЧЕВЫЕ СЛОВА: радиолокационный измерительный комплекс; космический объект; кластерный анализ; невязка измерений.

Сведения об авторах:

[1] заместитель директора департамента создания ситуационных центров и автоматизированных систем управления АО «Кронштадт технологии», г. Санкт-Петербург, Россия, nurkon@yandex.ru

[2] начальник лаборатории военного института (научно-исследовательского) Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, vka@mil.ru

[3] к.т.н., доцент, старший научный сотрудник лаборатории военного института (научно-исследовательского) Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, vka@mil.ru

Для цитирования: *Кондыбаев Н.С., Куприянов Н.А., Куракин С.З.* Алгоритм траекторной обработки информации радиолокационных измерительных комплексов на основе кластеризации методом K-MEANS // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 4–10. doi: 10.36724/2409-5419-2020-12-6-4-10

Ведение

В настоящее время наблюдаются интенсивные процессы техногенного засорения околоземного космического пространства (ОКП) вследствие увеличения числа космических объектов (КО). Деятельность человеческой цивилизации по освоению космоса привела к тому, что в ОКП помимо действующих космических аппаратов также находятся прекратившие работу спутники, разгонные блоки и элементы космического мусора [1]. Это ведёт как к повышенному риску столкновений КО, так и к ограничениям на использование орбитального ресурса в интересах систем локации, навигации, дистанционного зондирования земной поверхности, телевидения и связи. С учётом прогнозируемого многократного увеличения количества КО в ОКП и уменьшения их размеров актуальной научно-технической задачей является решение вопроса повышения точности определения средствами наблюдения местоположения КО [2].

Координатная информация о местоположении значительного количества КО, расположенных на низких и средних околоземных орбитах, рассчитывается с применением различных радиолокационных измерительных комплексов (РЛК), определяющих мгновенное положение КО и рассчитывающих траектории их движения. Для достижения большей точности прогнозирования опасных сближений КО необходимо как можно более правильно рассчитать его параметры движения, что может быть достигнуто, в первую очередь, за счёт повышения точности единичного измерения координат КО.

Для решения задачи повышения точности единичного измерения координат КО необходимо рассмотреть причины возникновения погрешностей измерений координат, выработать предложения по компенсации ошибок измерений и разработать научно-методический аппарат, реализующий предлагаемый способ повышения точности траекторных измерений РЛК.

Основные причины возникновения погрешностей измерений РЛК местоположения КО кратко рассмотрены ниже.

Основные причины погрешности измерений координат космических объектов

Повышение точности единичного измерения РЛК достигается за счёт компенсации погрешностей измерений. Как правило, в зависимости от причины возникновения ошибки разделяются на аппаратурные, методические и атмосферные, вызванные влиянием среды распространения радиоволн [3]

$$\delta_{rad} = \delta_{rad}^{atm} + \delta_{rad}^{app} + \delta_{rad}^{met}.$$

При этом опыт создания и эксплуатации различных РЛК показал [3, 4], что дальнейшее повышение их точностных характеристик может быть обеспечено в первую очередь за счёт компенсации негативного влияния среды распространения радиоволн, происхождение которого носит естественный или искусственный характер [5, 6].

Влияние среды распространения на точностные характеристики различных РЛК различается и в наиболее общем случае зависит от параметров используемых радиосигналов. При этом, по существующим оценкам [3, 4], наибольший вклад в атмосферные погрешности измерений приходится на тропосферную δ_{rad}^{trp} и ионосферную δ_{rad}^{ins} составляющие

$$\delta_{rad}^{atm} = \delta_{rad}^{trp} + \delta_{rad}^{ins}.$$

Величина тропосферной составляющей зависит от температуры, давления и влажности в месте размещения РЛК, а величина ионосферной составляющей определяется электронной концентрацией <<K_Eqn005.eps>> пересекаемых зондирующими и отражёнными радиосигналами слоёв ионосферы

$$\delta_{rad}^{ins} = f(N_e).$$

При этом N_e имеет регулярную N_e^{rg} и спорадическую N_e^{sp} составляющие

$$N_e = N_e^{rg} + N_e^{sp}$$

Вариации N_e^{rg} зависят от времени года и суток, что на практике позволяет достаточно хорошо описывать их в различных эмпирических моделях [3]. Вариации N_e^{sp} проявляются вследствие причин естественного и искусственного происхождения, поэтому прогнозировать время их возникновения и параметры перемещения практически невозможно. В то же время, рядом научно-исследовательских организаций накоплен значительный объём статистических данных о пространственно-временных параметрах некоторых видов ионосферных явлений, ведущих к изменению N_e^{sp}, а именно: размер, время существования, относительное изменение полного электронного содержания и N_e [6, 7].

Исследования ряда авторов показали [8, 9], что применяемые подходы к компенсации δ_{rad}^{ins} основаны на расчёте N_e^{rg} по усреднённым модельным значениям. Такое решение позволяет достигать приемлемую точность измерений в спокойных гелиогеофизических условиях (ГГФУ), когда величиной N_e^{sp} можно пренебречь вследствие её минимального значения. Для адаптации моделей к реальным ГГФУ используются данные оперативного мониторинга, поступающие от различных средств. Наиболее широко применяемым в настоящее время источником данных оперативного мониторинга являются измерения полного электронного содержания, рассчитываемые по сигналам навигационных спутников систем *GPS* и ГЛОНАСС [10].

Исследования [11] показали, что ограниченное количество навигационных спутников не позволяет проводить мониторинг имеющих широкие угловые размеры зоны обзора РЛК с высоким пространственным и временным разрешением. В результате по мере удаления от радиолиний навигационных спутников возникают области отсутствия данных, значения N_e в которых описываются модельными параметрами. В случае значительных вариаций N_e^{sp} РЛК проведёт измерение координат КО с некомпенсированной погрешностью. При проведении нескольких таких измерений возможно возникновение ошибок первого и второго рода при принятии решения о наличии или отсутствии КО, что негативно снижает информационные возможности РЛК.

В наиболее общем случае, к таким же отрицательным результатам приводит и локация цели в условиях активного помехового воздействия. Рост погрешностей измерений по зоне обзора РЛК увеличивается по мере приближения к границам центра источника активной помехи. При этом, в зависимости от характеристик РЛК и параметров помехоносителя, локация цели в центре источника активной помехи практически невозможна по причине отсутствия корреляционных связей между излучённым и полученными сигналами.

При этом в обоих описанных выше случаях невязки измерений местоположения КО, по которым имеется априорная координатная информация, в настоящее время не учитываются. Поэтому возникла идея по использованию невязок измерений для определения факта и параметров внешнего воздействия на точность единичного измерения РЛК координат КО.

Предложения по использованию невязки измерений координат космических объектов

Предлагается использовать невязки измерений для решения обратной задачи, суть которой заключается в следующем: при проведении компарирования (сравнения с величиной априорно известного оригинала) результатов измерения координат КО определяются параметры внешней среды в соответствующем направлении, которые используются при обработке координатной информации по другим близко расположенным КО.

Для практической реализации предлагаемого способа компенсации погрешностей траекторных измерений может быть использована измеренная РЛК дальность до КО r_{rad}^i и априорно известная дальность до наблюдаемого КО r_{apr}^i при выполнении условия:

$$\left| r_{rad}^i - r_{apr}^i \right| < \delta_{rad}^r, \qquad (1)$$

где δ_{rad}^r — допустимая конструкционная погрешность измерения дальности РЛК.

Для проверки работоспособности предлагаемого способа проведено моделирование процесса сопровождения КО расположенным вблизи города Горно-Алтайск РЛК с параметрами: $r_{rad} = 4000$ км, $\beta_{rad} = 80°$, $\varepsilon_{rad} = 40°$, $\delta_{rad}^r = 50$ м. Для моделирования использованы баллистические начальные данные формата *TLE* и математическая модель движения *SGP*4 [12]. При этом полагалось, что находящиеся в зоне обзора РЛК ионосферные неоднородности неподвижны и изменяют N_e^{sp} в своих границах, что ведёт к увеличению длины траекторий радиосигналов и, как следствие, росту погрешностей измерения дальности. Результатом моделирования является множество измерений координат каталогизированных КО в зоне обзора РЛК. На рис. 1 представлено распределение измерений координат КО на β-ε проекции зоны обзора 21 июня 2020 года для периода времени 18:00–18:05 с временным интервалом 6 с. Знаком ○ отмечено положение КО на момент измерения, а знаком ● последнее полученное по КО измерение перед окончанием времени моделирования или выходом КО из зоны обзора РЛК.

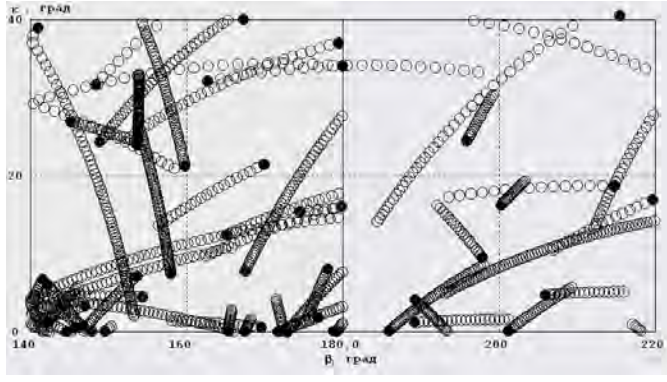

Рис. 1. Положение КО на β-ε проекции зоны обзора моделируемого РЛК

Затем проводилось моделирование процесса возникновения погрешности измерения дальности для тех КО, положение которых относительно РЛК предполагает прохождение зондирующим и отражённым сигналами ионосферных неоднородностей. В результате ряд измерений дальности до КО переставал удовлетворять выражению (1). Результаты моделирования представлены на рис. 2, при этом для удобства отображения проекция представлена дискретезированной с шагом в 1°. Положение КО при условии выполнения выражения (1) обозначено знаком ■, а знаком ■ — при условии невыполнения.

Результаты моделирования показали, что влияние ионосферных неоднородностей ведёт к увеличению δ^r для множества КО, находящихся в соответствующем β-ε направлении. Для представленного на рисунке 2 распре-

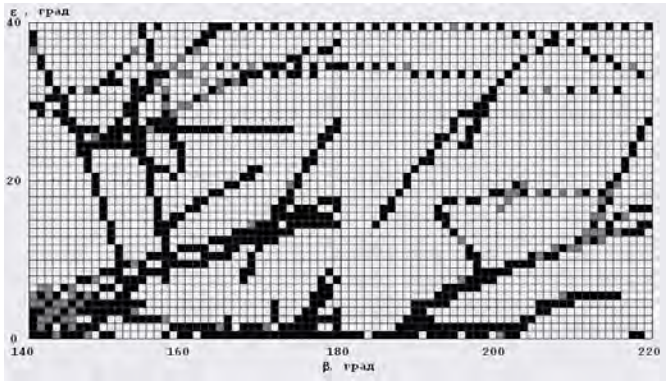

Рис. 2. Положение КО на дискретезированной β-ε проекции зоны обзора моделируемого РЛК

деления КО достаточно хорошо прослеживаются 3 группы измерений с погрешностями, находящиеся на 140…150°, 159…71° и 195…215° азимута соответственно.

Кроме того, имеются разрозненные измерения, которые в явном виде не могут быть отнесены к какой-либо из этих групп. Для принятия решения о принадлежности данных измерений к группе авторами статьи разработан алгоритм, основанный на использовании методов кластерного анализа, а именно метода *K-MEANS*. Ниже представлены основные этапы разработанного алгоритма.

Основные этапы алгоритма кластеризации методом *K-MEANS*

Алгоритм кластеризации методом *K-MEANS* включает следующие этапы:

1. РЛК производит измерение координат КО в зоне обзора на момент периода обзора:

$$M = \left\{ \vec{m}_1, \vec{m}_2, ..., \vec{m}_j \right\},$$

$$\vec{m}_j = \left\langle t_j, r_j, \beta_j, \varepsilon_j \right\rangle,$$

где t_j — время проведения измерения;
r_j — дальность КО, км;
β_j — азимут КО, °;
ε_j — угол места КО, °.

2. РЛК проводит компарирование результатов измерения дальности с априорной координатной информацией, формируя массив измерений *F*, не удовлетворяющих выражению (1):

$$F = \left\{ \vec{f}_1, \vec{f}_1, ..., \vec{f}_i \right\},$$

$$\vec{f}_i = \left\langle t_i, r_i, \beta_i, \varepsilon_i \right\rangle.$$

При этом возможно накопление измерений в течение нескольких периодов обзора — например, на время квазистабильности ионосферы [13] или предполагаемой длительности помехового воздействия.

3. РЛК формирует множество измерений *C*, принимаемых как начальные центры кластеров

$$C = \left\{ \vec{c}_1, \vec{c}_2, ..., \vec{c}_a \right\},$$

$$\vec{c}_a = \left\langle t_a, r_a, \beta_a, \varepsilon_a \right\rangle,$$

$$C \cap F.$$

Исходя из известных размеров ионосферных неоднородностей, измерения внутри одного кластера должны быть распределены не более чем на *x*° по азимуту и *y*° углу места

$$\left| \beta_a - \beta_{a+1} \right| < x,$$
$$\left| \varepsilon_a - \varepsilon_{a+1} \right| < C$$

При этом полагается, что в одном кластере должно находиться не менее 5 измерений. На данном этапе отфильтровываются разрозненные измерения, которые явно не могут быть следствием влияния ионосферной неоднородности.

На рис. 3 представлена β-ε проекция зоны обзора моделируемого РЛК, описывающая соответствующее рисункам 1 и 2 положение КО с обозначением начальных центров кластеров 1, 2 и 3.

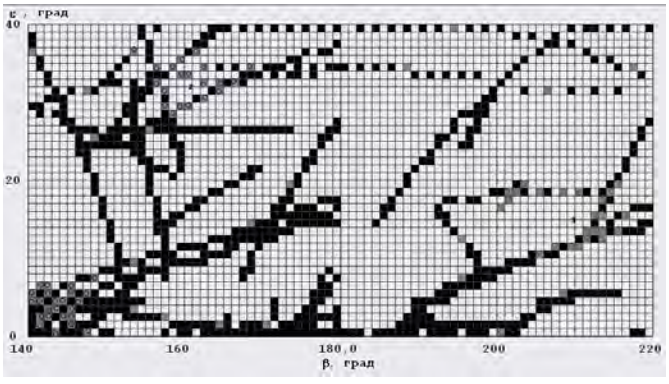

Рис. 3. Положение КО на дискретезированной β-ε проекции зоны обзора моделируемого РЛК с обозначением начальных центров кластеров

4. РЛК рассчитывает распределение измерений по кластерам

$$\forall \vec{f}_i \in F, i = 1, 2, ..., n,$$

$$\vec{f}_i \in S_k \Leftrightarrow k = \arg\min_a p\left(\vec{f}_i, \vec{c}_a^{(t-1)} \right)^2.$$

5. РЛК производит пересчёт центров кластеров

$$\vec{c}_i^{(t)} = \frac{1}{|S_i|} \sum_{\vec{f}_i \in S_i} \vec{f}_i, \forall i = 1, 2, ..., a.$$

6. Окончание расчёта при обработке всех имеющихся измерений F, не удовлетворяющих выражению (1)

$$f_{i+1} = 0.$$

Результатом расчёта является множество измерений, объединённых в несколько кластеров и описывающее пространственно-временное распределение невязок измерений в зоне обзора РЛК.

На рис. 4 представлена β-ε проекция зоны обзора моделируемого РЛК, описывающая соответствующее рисунках 1–3 положение КО с обозначением кластеров 1, 2 и 3, рассчитанных в результате выполнения этапов алгоритма.

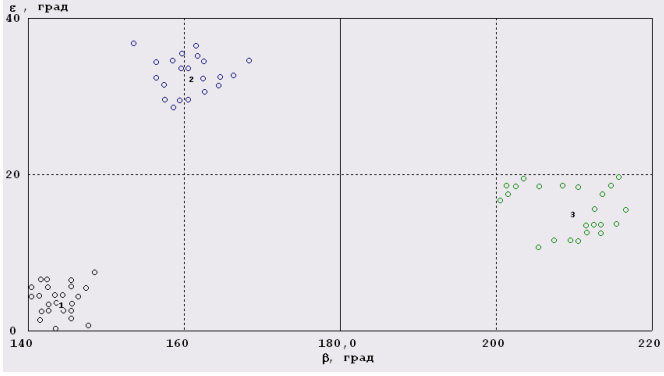

Рис. 4. Расположение кластеров КО на β-ε проекции зоны обзора моделируемого РЛК

Рассчитанные кластеры КО могут быть использованы для последующей обработки координатной информации о других КО, по которым получены измерения местоположения в границах соответствующих кластеров, а априорная координатная информация о них отсутствует. Для этого могут быть использованы общеприменимые подходы, используемые в различных моделях среды распространения радиоволн [8, 10].

При этом одним из перспективных направлений предметной области статьи является учёт местоположения навигационных спутников при формировании рассматриваемых кластеров, что позволит, в случае реализации, проводить мониторинг зоны обзора РЛК с более высоким временным и пространственным разрешением, исключая возникновение областей отсутствия данных [14].

Таким образом, предложенный способ на основе реализации алгоритма кластеризации методом *K-MEANS* позволяет повысить точность траекторных измерений космических объектов за счет учета невязок измеренных и априорно известных координат КО, находящихся в сформированных кластерах зоны обзора РЛК.

Заключение

Предложенный в статье алгоритм траекторной обработки на основе кластеризации методом *K-MEANS* позволяет по невязкам измеренных и априорно известных координат КО, находящихся в зоне обзора РЛК, сформировать кластеры измерений. Такое решение позволяет отфильтровать неизбежно возникающие разрозненные измерения, содержащие погрешности, которые не могут быть следствием внешнего воздействия, вызванного изменением ГГФУ или активным помеховым воздействием. При получении измерений координат не имеющих априорной координатной информации КО рассчитанные границы кластеров позволят учесть пространственно-временную неопределённость погрешностей измерений, вызванных внешним влиянием. В условиях роста числа КО в ОКП предложенное решение позволит повысить точность определения координат КО в современных РЛК траекторной обработки, что благоприятно скажется на их информационных возможностях. При этом реализация рассмотренной идеи в современных РЛК требует лишь заблаговременного наличия априорной координатной информации о наблюдаемых КО, а также проведения доработки программного обеспечения обработки координатной информации.

Литература

1. *Архипов В.А., Булынин Ю.Л., Гафаров А.А., Головко А.В., Горлов А.Е.* Космический мусор. Книга 2. Предупреждение образования космического мусора: монография. М.: Физматлит, 2014, 188 с. ISBN: 978–5–9221–1504–9.

2. *Олейников И.И., Астраханцев М.В.* Способ построения расширенного каталога космических объектов размерами более 1 см на основе базы данных АСПОС ОКП // Решетневские чтения (Красноярск, 12–14 ноября 2013 г.). 2013. С. 37–39. ISSN: 1990–7702.

3. *Оводенко В.Б., Трёкин В.В.* Исследование эффективности компенсации влияния среды на работу радиолокационной станции // Труды Московского авиационного института. 2015. № 88. С. 52–67. eISSN: 1727–6942.

4. *Аксенов О.Ю., Боев С.Ф., Виноградов А.Г., Лучин А.А., Потехин А.П.* Проблемные вопросы создания системы прогноза геогелиофизических условий функционирования радиолокационных станций дальнего обнаружения // XXIV Всероссийская научная конференция «Распространение радиоволн» (Иркутск, 29 июня-05 июля 2014 г). 2014. Том IV, Секция 6. С. 5–8.

5. *Черногор Л.Ф., Фролов В.Л.* Перемещающиеся ионосферные возмущения, генерируемые периодическим нагревом околоземной плазмы радиоизлучением стенда «Сура» // XXIV Всероссийская научная конференция «Распространение радиоволн» (Иркутск, 29 июня-05 июля 2014 г). 2014. Том IV, Секция 6. С. 104–107.

6. *Афраймович Э.Л., Воейков С.В., Лесюта О.С., Перевалова Н.П., Нагорский П.М.* Перемещающееся ионосферное возмущение, возможно, инициированное высотным взрывом // Солнечно-земная физика. 2003. № 3 (116). С. 73–79.

7. *Шерстюков Р.О., Ачкурин А.Д.* Анализ дневных среднемасштабных перемещающихся ионосферных возмущений по двумерным картам вариаций полного электронного содержания и ионограмм // Учёные записки Казанского (Поволжского) федерального университета. 2017. Т. 159, Кн. 3. С. 374–389.

8. *Ясюкевич Ю.В., Оводенко В.Б., Мыльникова А.А., Живетьев И.В., Веснин А.М., Едемский И.К., Котова Д.С.* Методы компенсации ионосферной составляющей ошибки радиотехнических систем с применением данных полного электронного содержания GPS/ГЛОНАСС // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и информационные системы. 2017. № 2 (34). С. 19–31. ISSN: 2306–2819.

9. *Колесник А.Г., Голиков И.А., Чернышев В.И.* Матема-тические модели ионосферы. Томск: МГП «Раско», 1993. 240 с.

10. *Котова Д.С., Захаров В.Е., Клименко М.В., Клименко В.В.* Влияние выбора модели среды на решение задачи распространения КВ-радиоволн // XXIV Всероссийская научная конференция «Распространение радиоволн» (Иркутск, 29 июня-05 июля 2014 г). 2014. Том IV, Секция 6. С. 121–125.

11. *Куприянов Н.А., Мисько Р.С.* Подход к использованию каталогизированных космических объектов в интересах потребителей навигационной информации // 75-я Всероссийская научно-техническая конференция, посвящённая Дню радио (Санкт-Петербург, 20–24 апреля 2020 г.). СПб., 2020. С. 36–39.

12. *Чагина В.А., Гришко Д.А., Майорова В.И.* Расчёт движения космического аппарата на околокруговой орбите по данным TLE по упрощённой модели SGP // Наука и образование. 2016. № 1. С. 52–66.

13. *Ясюкевич Ю.В., Живетьев И.В., Ясюкевич А.С., Воейков С.В., Захаров В.И., Перевалова Н.П., Титков Н.Н.*Влияние ионосферной и магнитосферной возмущённости на сбои глобальных навигационных спутниковых систем // Современные проблемы дистанционного зондирования Земли из космоса. 2017. Т. 14. № 1. С. 88–98.

14. *Куницын В.Е., Нестерова И.А., Андреева Е.С.* Радиотомографические исследования ионосферы по данным навигационных спутниковых систем // Всероссийские научные Зворыкинские чтения — VI (Муром, 14 февраля 2014 г.). 2014. С. 12–19.

ALGORITHM FOR TRAJECTORY INFORMATION PROCESSING OF RADAR MEASURING COMPLEXES BASED ON K-MEANS CLUSTERING

NURLAN S. KONDIBAEV
St. Petersburg, Russia, nurkon@yandex.ru

NIKOLAY A. KUPRIYANOV
St. Petersburg, Russia, vka@mil.ru

SERGEY Z. KURAKIN
St. Petersburg, Russia, vka@mil.ru

KEYWORDS: radar measuring complex; space object; cluster analysis; the discrepancy of measurements.

ABSTRACT

The problem situation caused by the need to improve the accuracy of determining the location of observed space objects by radar measuring complexes is considered. It is shown that the accuracy characteristics of radar measuring systems depend on the contribution of various measurement errors, the most significant of which for modern highly informative observation tools are atmospheric, determined by heliogeophysical conditions of operation. It is noted that the currently applied approaches to compensation of atmospheric measurement errors do not allow taking into account the heliogeophysical conditions of operation of radar measuring complexes with high time and spatial resolution. It is shown that when processing coordinate information, sporadic changes in heliogeophysical operating conditions are not fully taken into account, which leads to an increase in errors in measuring the location of space objects and a decrease in the information capabilities of radar measuring complexes. The idea of using the discrepancy of measurements by the radar measuring complex of the location of space objects for which there is a priori coordinate information is considered. The results of combining groups of space object location measurements using cluster analysis methods are shown. The results of computer modeling are presented and it is shown that the proposed approach allows us to determine the areas where the influence of heliogeophysical conditions increases the measurement errors. The main calculation relations are described and the stages of the algorithm for trajectory processing of information from radar measuring complexes based on clustering by the K-MEANS method are shown. Further directions of using the results of the algorithm are proposed, which consist in using data on formed clusters for processing information about space objects for which there is no a priori coordinate information. It is shown that the proposed approach can be applied in order to improve the information capabilities of radar measuring systems.

REFERENCES

1. Arhipov V.A., Bulynin Ju. L., Gafarov A.A., Golovko A.V., Gorlov A.E. *Kosmicheskij musor. Kniga 2. Preduprezhdenie obrazovanija kosmicheskogo musora: monografija* [Space debris. Book 2. Prevention of space debris: a monograph]. M.: Fizmalit, 2014, 188 p. ISBN: 978–5–9221–1504–9. (In Rus)
2. Olejnikov I.I., Astrahancev M.V. The way to create the catalogue for bigger-than-1cm space objects based on the aspos okp database. *Reshetnevskie chtenija* [Reshetnev readings, Krasnoyarsk, November 12–14, 2013]. 2013. Pp. 37–39. ISSN: 1990–7702. (In Rus)
3. Ovodenko V.B., Trjokin V.V. Issledovanie jeffektivnosti kompensacii vlijanija sredy na rabotu radiolokacionnoj stancii [Study of the effectiveness of compensation for the influence of the environment on the operation of the radar station]. *Trudy Moskovskogo aviacionnogo instituta* [Proceedings of the Moscow aviation Institute]. 2015. № 88. Pp. 52–67. eISSN: 1727–6942. (In Rus)
4. Aksenov O. Yu., Boev S.F., Vinogradov A.G., Luchin A.A., Potekhin A.P. Challenges of creation of a forecasting system of geo-heliophysical conditions required for operation of superlong-range radar systems. *XXIV Vserossijskaja nauchnaja konferencija "Rasprostranenie radiovoln"* [XXIV all-Russian scientific conference "radio wave propagation" (Irkutsk, June 29-July 05, 2014)]. 2014. Vol. IV, Section 6. Pp. 5–8. (In Rus)
5. Chernogor L.F., Frolov V.L. Peremeshhajushhiesja ionosfernye vozmushhenija, generiruemye periodicheskim nagrevom okolozemnoj plazmy radioizlucheniem stenda «Sura» [Moving ionospheric disturbances generated by periodic heating of near-earth plasma by radio emission from the Sura stand»]. *XXIV Vserossijskaja nauchnaja konferencija "Rasprostranenie radiovoln"* [XXIV all-Russian scientific conference "radio wave propagation" (Irkutsk, June 29-July 05, 2014)]. 2014. Vol. IV, Section 6. Pp. 104–107. (In Rus)
6. Afraimovich E.L., Voeykov S.V., Lesyuta O.S., Perevalova N.P., Nagorsky P.M. The traveling ionospheric disturbance conceivably initiated by a high altitude explosion. *Solnechno-zemnaja fizika* [Solar-terrestrial physics]. 2003. Vol 3. Pp. 73–79. (In Rus)
7. Sherstjukov R.O., Achkurin A.D. Analysis of Daytime Medium-Scale Traveling Ionospheric Disturbances by Two-Dimensional Maps of Total Electron Content Perturbation and Ionograms. *Uchenye zapiski kazanskogo universiteta. Seriya fiziko-matematicheskie nauki* [Proceedings of Kazan University. Physics and Mathematics Series]. 2017. Vol. 159, Book 3. Pp. 374–389. (In Rus)
8. Yasyukevich Yu.V., Ovodenko V.B., Mylnikova A.A., Zhivetiev I.V., Vesnin A.M., Edemskiy I.K., Kotova D.S. GPS/GLONASS total electron content based methods for ionospheric error compensation for the radio communication systems. *Vestnik Povolzhskogo gosudarstvennogo tehnologicheskogo universiteta. Ser.: Radiotehnicheskie i informacionnye sistemy* [Bulletin of the Volga state technological University. Series: Radio engineering and information systems]. 2017. № 2 (34). Pp. 19–31. ISSN: 2306–2819. (In Rus)
9. Kolesnik A.G., Golikov I.A., Chernyshev V.I. *Matematicheskie modeli ionosfery* [Mathematical models of the ionosphere]. Tomsk: MGP «Rasko», 1993. 240 p. (In Rus)
10. Kotova D.S., Zaharov V.E., Klimenko M.V., Klimenko V.V. Vlijanie vybora modeli sredy na reshenie zadachi rasprostranenija KV-radiovoln [Influence of the choice of the medium model on the solution of the problem of HF radio wave propagation]]. *XXIV Vserossijskaja nauchnaja konferencija "Rasprostranenie radiovoln"* [XXIV all-Russian scientific conference "Radio wave propagation", Irkutsk, June 29-July 05, 2014]. 2014. Vol. IV, Section 6. Pp. 121–125. (In Rus)
11. Kuprijanov N.A., Mis'ko R.S. Podhod k ispol'zovaniju katalogizirovannyh kosmicheskih ob'ektov v interesah potrebitelej navigacionnoj informacii [Approach to using cataloged space objects for the benefit of navigation information consumers]. *75-Ja Vserossijskaja nauchno-tehnicheskaja konferencija, posvjashhjonnaja Dnju radio* [75th all-Russian scientific and technical conference dedicated to radio day, Saint Petersburg, April 20–24, 2020]. 2020. Pp. 36–39. (In Rus)
12. Chagina V.A., Grishko D.A., Majorova V.I. Raschjot dvizhenija kosmicheskogo apparata na okolokrugovoj orbite po dannym TLE po uproshhjonnoj modeli SGP [Calculation of the spacecraft's motion in a near-circular orbit based on TLE data using the simplified SGP model]. *Nauka i obrazovanie* [Science and education]. 2016. No. 1. Pp. 52–66. (In Rus)
13. Yasyukevich Yu.V., Zhivetiev I.V., Yasyukevich A.S., Voeykov S.V., Zakharov V.I., Perevalova N.P., Titkov N.N. Ionosphere and magnetosphere disturbance impact on operation slips of global navigation satellite systems. *Sovremennye problemy distancionnogo zondirovanija Zemli iz kosmosa* [Modern problems of remote sensing of the Earth from space]. 2017. Vol 14. No. 1. Pp. 88–98. (In Rus)
14. Kunicyn V.E., Nesterova I.A., Andreeva E.S. Radiotomograficheskie issledovanija ionosfery po dannym navigacionnyh sputnikovyh system [Radio-tomographic studies of the ionosphere according to navigation satellite systems]. *Vserossijskie nauchnye Zvorykinskie chtenija* ["All – Russian scientific Zvorykin readings-VI", Murom, February 14, 2014]. 2014. Pp. 12–19. ISSN: 2222–2979. (In Rus)

INFORMATION ABOUT AUTHORS:

Kondibaev N.S., Deputy Director of the department for creating situation centers and automated control systems JSC «Kronshtadt technologies».

Kupriyanov N.A., Head of the military institute (research) of Mozhaisky Military Space Academy.

Kurakin S.Z., PhD, Docent, Senior research officer of the laboratory of the military institute (research) of Mozhaisky Military Space Academy.

For citation: Kondibaev N.S., Kupriyanov N.A., Kurakin S.Z. Algorithm for trajectory information processing of radar measuring complexes based on K-MEANS clusteringe. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 4–10. doi: 10.36724/2409-5419-2020-12-6-4-10 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-11-17

АДАПТИВНОЕ УСТРОЙСТВО ПРЕДЫСКАЖАЮЩЕЙ ЛИНЕАРИЗАЦИИ ДЛЯ БОРТОВЫХ РАДИОПЕРЕДАЮЩИХ УСТРОЙСТВ

ПЕТУШКОВ
Сергей Владимирович

АННОТАЦИЯ

Улучшение энергетических и спектральных характеристик бортовых радиопередающих устройств, функционирующих в жестких условиях космического пространства, с помощью систем предыскажающей линеаризации становиться все более актуальной задачей. Предложенное адаптивное устройство предыскажающей линеаризации, основано на корреляционной оценке уровня нелинейных искажений на выходе усилителя мощности. Данное устройство позволяет обеспечить более высокую эффективность линеаризации при меняющихся характеристиках бортового радиопередающего устройства в процессе длительного функционирования космического аппарата на орбите, в отличие от систем с предварительной настройкой. Предложенное техническое решение имеет более высокие показатели надежности и упрощенную техническую реализацию по сравнению с аналогами за счет отсутствия предварительной аналоговой и цифровой обработки СВЧ-сигнала. Для моделирования работы адаптивного устройства предыскажающей линеаризации был разработан простой алгоритм, занимающий меньшую логическую емкость цифровых микросхем, по сравнению с известными методами адаптации. Предложенный алгоритм требует меньше математических вычислений за один цикл итерации, основанный на определении направления роста градиента взаимно корреляционной функции, по которому будет происходить изменение параметров предыскажающего линеаризатора. Результаты моделирования предложенного адаптивного устройства предыскажающей линеаризации показывают, что процесс двумерной адаптации на основе разработанного алгоритма однозначен и приводит к восстановлению оптимальной настройки его нелинейных характеристик. Адаптационный процесс приводит к снижению уровня интермодуляционных искажений на выходе усилителя мощности за несколько циклов адаптации. Так же стоит отметить, что процесс оптимизации и подбора двух параметров предыскажающего линеаризатора в составе усилителя мощности происходит одинаково, независимо от того, использована аналоговая или цифровая реализация линеаризатора.

Сведения об авторе:

к.т.н., ассистент кафедры Национального исследовательского университета «Московский энергетический институт», ведущий инженер-исследователь АО «Российские космические системы», г. Москва, Россия, petushkov.sv@spacecorp.ru

КЛЮЧЕВЫЕ СЛОВА: радиопередающее устройство; усилитель мощности; интермодуляционные искажения; адаптивный линеаризатор; предыскажающая линеаризация; взаимно корреляционная функция.

Для цитирования: *Петушков С.В.* Адаптивное устройство предыскажающей линеаризации для бортовых радиопередающих устройств // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 11–17. doi: 10.36724/2409-5419-2020-12-6-11-17

Введение

В настоящее время для выполнения требований к высокой спектральной эффективности при разработке бортовых радиопередающих устройств используются сложные типы модуляции формируемых сверхвысокочастотных (СВЧ) сигналов[1,2]. При прохождении таких сигналов через усилитель мощности, функционирующий в энергетически эффективном режиме вблизи насыщения активного элемента, возникают сильные нелинейные искажения на выходе усилителя, ухудшающие качество передаваемой информации в рабочей полосе частот и нарушающие требования электромагнитной совместимости (ЭМС) за её пределами. В связи с повышенным требованием по энергетической эффективности метод снижения уровня выходной мощности усилителя относительно точки насыщения, для монохроматического сигнала, позволяющий снизить уровень нелинейных искажений до допустимого, становится неприменим. Для решения данной проблемы, при разработке радиопередающих устройств, все большее применение находят устройства предыскажающей линеаризации характеристик усилителей мощности [1–6].

Однако функционирование усилителя мощности в составе бортового радиопередающего устройства в жестких условиях космического пространства, где он подвержен влиянию дестабилизирующих внешних воздействующих факторов: ионизирующего излучения космического пространства и изменению температуры; использование схем предыскажающей линеаризации с предварительной настройкой не может полностью обеспечивать высокую эффективность линеаризации.

Для решения данной проблемы разрабатываются системы с адаптацией параметров линеаризатора под изменяющиеся характеристики усилителя мощности в процессе его эксплуатации [7–10].

Реализация предложенных схем в основном применима к наземной аппаратуре (системы телерадиовещания, сотовая связь и т.д.) и требует введения в состав радиопередающего устройства дополнительных устройств демодуляции СВЧ-сигналов, устройств цифровой обработки (АЦП — аналогово-цифровой преобразователь, ПЛИС — программируемая логическая интегральная схема, МК — микроконтроллер). Использование этих схем применительно к бортовому радиопередающему устройству ухудшит его показатели надежности и потребует введения сложных и объемных алгоритмов адаптационных вычислений в блоки цифровой обработки сигнала, требующих большей логической ёмкости используемых цифровых микросхем.

Постановка задачи и алгоритм работы устройства

Для устранения вышеописанных проблем предлагается использование следующей технической реализации адаптивного устройства предыскажающей линеаризации, основанной на корреляционной оценке уровня нелинейных искажений на выходе усилителя мощности, представленной на рис. 1.

Основной принцип, на котором основана работа данной адаптивной предыскажающей системы, заключается в формировании взаимно корреляционной функции, показываю-

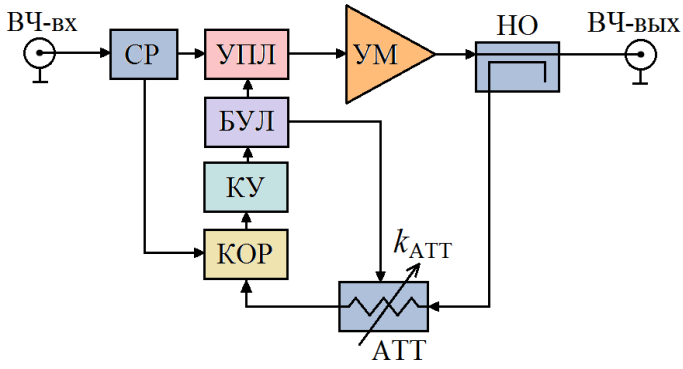

Рис. 1. Линеаризованный усилитель мощности с адаптивным устройством предыскажающей линеаризации: СР — сумматор-разветвитель; УПЛ — устройство предыскажающей линеаризации; НО — направленный ответвитель; БУЛ — блок управления линеаризатором; КУ — квантователь уровня; КОР — коррелятор; АТТ — аттенюатор

щей степень идентичности между входным СВЧ-сигналом предыскажающего линеаризатора и выходным искаженным СВЧ-сигналом усилителя мощности, сдвинутых на время τ друг относительно друга. Время τ определяет задержку выходного СВЧ-сигнала усилителя относительного входного сигнала предыскажающего линеаризатора.

При отсутствии нелинейных искажений сигналы на выходе усилителя мощности и входе линеаризатора будут идентичны и взаимно корреляционная функция будет нарастать до своего максимального значения. При появлении нелинейных искажений на выходе усилителя мощности максимальное значение взаимно корреляционной функции будет уменьшаться тем больше, чем выше уровень нелинейных искажений.

Критерий оценки взаимно корреляционной функции очень удобен для автономного бортового радиопередающего устройства, так как позволяет количественно оценить текущий уровень нелинейных искажений при вариациях параметров усилителя мощности без демодуляции СВЧ-сигнала и последующей цифровой обработки. В предложенной схеме, данные операции реализуются в аналоговом виде в бло-

[1]Бартенев В. А., Кантор Л. Я. и др. Спутниковая связь и вещание: справочник / под ред. Л. Я. Кантора. 3-е изд. М.: Радио и связь. 1997. 528 с.

[2]Скляр Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ. 2-е изд. М.: Вильямс,2003. 1104 с.

ке коррелятора и квантователя уровня. Такое построение адаптивного устройства предыскажающей линеаризации имеет более простую схемотехническую реализацию на практике в отличие от современных методов адаптации, используемых при реализации адаптивных устройств цифрового предыскажения [7–10], основанных на минимизации целевой функции, путем изменения параметров линеаризатора (метод стохастического градиента, рекурсивный метод наименьших квадратов и. др.).

Принцип работы схемы на рис. 1 состоит в следующем. В блоке коррелятора вычисляется взаимно корреляционная функция[3] [11] между входным сигналом предыскажающего линеаризатора и выходным искаженным сигналом усилителя мощности и поступает на вход квантователя уровня. С выхода квантователя сигнал поступает в блок управления линеаризатором, в котором устанавливается определённое значение порогового уровня взаимно корреляционной функции ($B_{пор}$), определяющее допустимый уровень интермодуляционных искажений на выходе усилителя мощности. Если текущий уровень взаимно корреляционной функции превышает допустимое значение, то блок управления линеаризатором не меняет параметры предыскажающего линеаризатора. В качестве регулируемых параметров линеаризатора выбираются параметры (p_1, p_2), отвечающие за подстройку его нелинейных характеристик. При увеличении уровня нелинейных искажений взаимно корреляционной функции, вычисленная в корреляторе, становится ниже порогового уровня $B_{пор}$ и блок управления линеаризатором запускает процесс подбора параметров линеаризатора, согласно алгоритму, представленному на рис. 2.

Управляемый аттенюатор необходим для ослабления сигнала с выхода направленного ответвителя, для выравнивания энергий сигналов поступающих на коррелятор, определяемых равенством Парсеваля.

Адаптация параметров линеаризатора (p_1, p_2) производится при помощи блока управления линеаризатором на вход которого поступает квантованный уровень вычисленной взаимно корреляционной функции в корреляторе (B_n). При предварительной настройке предыскажающего линеаризатора под конкретный усилитель мощности значения параметров $p_1 = p_{10}$ и $p_2 = p_{20}$ задаются как исходные, при которых достигается наилучший выигрыш по интермодуляционным искажениям на выходе усилителя.

После снижения взаимно корреляционной функцией порогового уровня $B_{пор}$ блок управления линеаризатором производит 8 шагов перебора параметров (p_1, p_2) с шагом Δpm, в окрестности исходных значений с запоминанием взаимно корреляционной функции (B_n) на каждом шаге итерации.

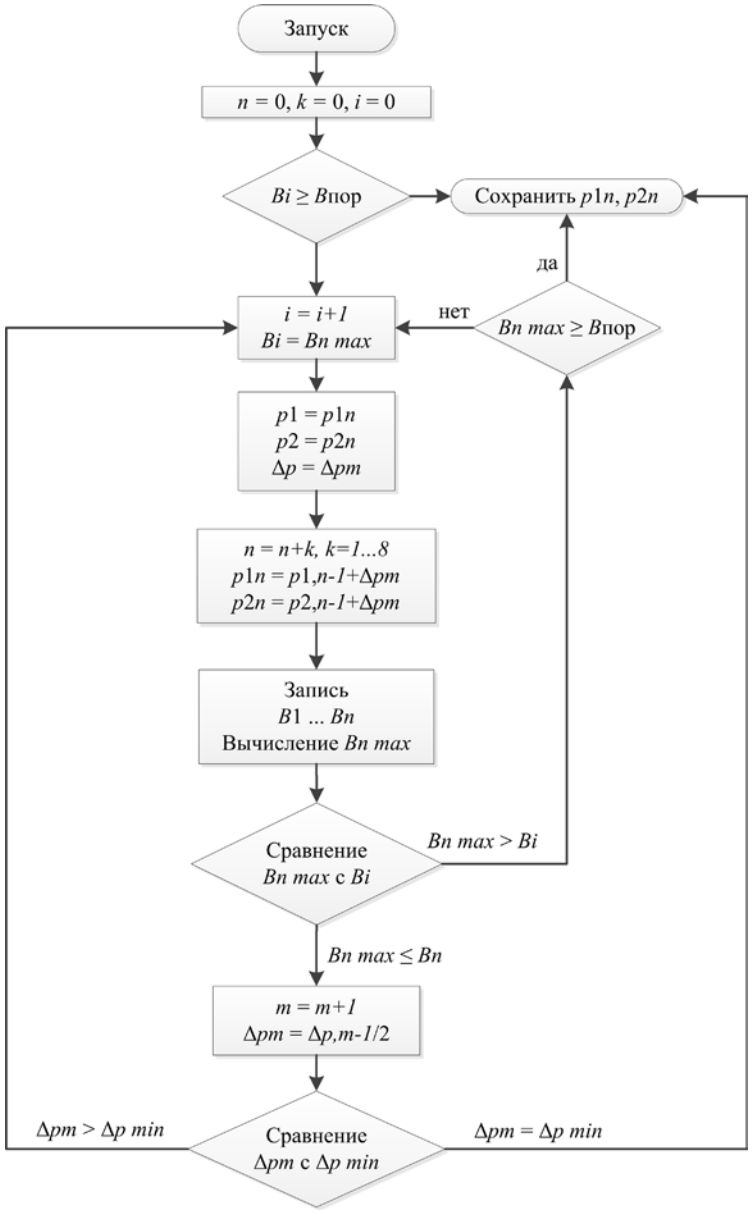

Рис. 2. Алгоритм работы блока управления адаптивного устройства предыскажающей линеаризации

Из полученного набора восьми значений B_n блок управления линеаризатором выбирает наибольшее, определяющее направление роста градиента по которому будет происходить дальнейшее изменение параметров (p_1, p_2) и которое займет наименьшее количество шагов итерации. После данной операции полученное сочетание параметров линеаризатора (p_1, p_2) и максимальное значение B_n сохраняются в памяти блока управления линеаризатором, и принимаются в качестве исходных для следующего шага итерации. Если перебор параметров линеаризатора (p_1, p_2) в блоке управления линеаризатором не приводит к увеличению взаимно корреляционной функции из 8 полученных

[3]Денисенко А. Н. Сигналы. Теоретическая радиотехника: справочное пособие. М.: Горячая линия – Телеком, 2005. 704 с.

значений B_n по сравнению с исходным на предыдущем шаге итерации, то происходит уменьшение шага изменения параметров вдвое.

Процесс адаптации параметров линеаризатора (p_1, p_2) заканчивается, если значение взаимно корреляционной функции B_n становится выше заданного в регистре порога $B_{пор}$, или шаг изменения параметров Δp_1, Δp_2 станет равным младшему значащему разряду микросхемы на которой реализован блок управления линеаризатором.

Найденные значения параметров линеаризатора (p_1, p_2) сохраняются на выходе блока управления линеаризатором до следующего процесса адаптации.

Таким образом, происходит подстройка характеристик амплитудной компрессии и амплитудно-фазовой конверсии в предыскажающем линеаризаторе под изменившиеся характеристики усилителя мощности и тем самым снижается уровень интермодуляционных искажений на выходе.

Результаты моделирования

Моделирование работы адаптивного устройства предыскажающей линеаризации проводилось в программной среде NI AWR Design Environment в подпрограмме Visual System Simulate (VSS). В качестве УПЛ использовалась модель аналогового предыскажающего линеаризатора [12], представленная на рис. 3.

Аналоговый предыскажающий линеаризатор состоит из линейной и нелинейной ветвей, разделяемых с помощью синфазных сумматоров-разветвителей (СР 1,2).

Нелинейная ветвь выполнена на гибридном кольце (ГК), к порту 3 которого подключена нелинейная ячейка на антипараллельных диодах Шоттки (ДШ1,2), а к порту 2 подключена RC-цепочка, представляющая собой фильтр нижних частот, частота среза которого много меньше несущей частоты f_0.

В состав линейной ветви, компенсирующей изменение амплитуды и фазового сдвига в нелинейной ветви аналогового предыскажающего линеаризатора, каскадно включены управляемые аттенюатор (АТТ) и фазовращатель (ФВ). Предварительная настройка данного аналогового предыскажающего линеаризатора осуществлялась с помощью выбора значений напряжения источника смещения диодов $E_{см}$, коэффициента усиления КУ линейного усилителя, уровня потерь $k_{атт}$ в аттенюаторе и фазового сдвига $\varphi_{ФВ}$ в фазовращателе.

В качестве параметров, изменяемых в процессе адаптации, аналогового предыскажающего линеаризатора выбирались значения напряжение смещения диодов Шоттки $p_1 = E_{см}$ и фазовый набег в фазовращателе $p_2 = \varphi_{ФВ}$. Управление параметрами осуществлялось блоком управления линеаризатором посредством выдачи соответствующих сигналов, поступающих на управляемый фазовращатель и источник питания. Изменение напряжения смещения диодов в источнике питания и набега фазы в фазовращателе подстраивает нелинейные характеристики амплитудной компрессии и амплитудно-фазовой конверсии аналогового предыскажающего линеаризатора под аналогичные изменившиеся характеристики усилителя мощности под действием того или иного внешнего воздействующего фактора в процессе эксплуатации. При подстройке нелинейных характеристик линеаризатора происходит изменение уровня интермодуляционных искажений на выходе усилителя мощности и тем самым происходит изменение взаимно корреляционной функции в блоке коррелятора.

В качестве модели усилителя мощности использовался электровакуумный усилитель, построенный на лампе бегущей волны, реализованной на имитационной модели Салеха [13]. Уровень интермодуляционных искажений в модели, для задания порогового значения ВКФ, оценивался по критерию мощности в соседнем канале (ACPR — Adjacent Channel Power Ratio) при тестовом входном сигнале с несущей частотой f_0 = 11,2 ГГц, 4-позиционной фазовой манипуляцией ФМ-4 по псевдослучайному закону со скоростью передачи информации 200 Мбит/с, с фронтами, сглаженными при помощи фильтра Найквиста [14].

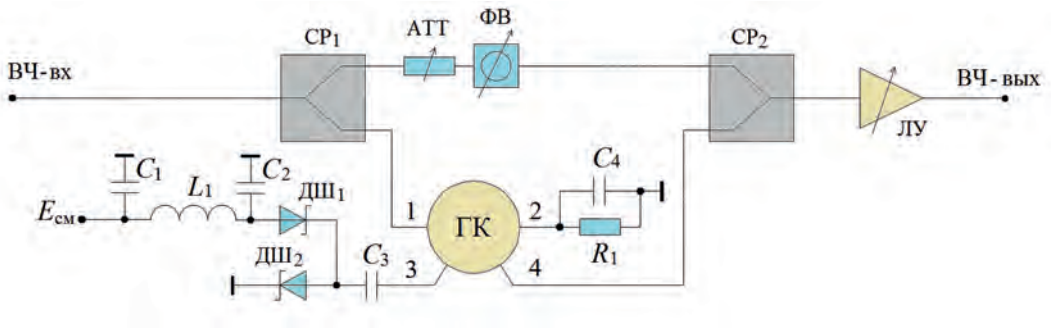

Рис. 3. Структурная схема аналогового предыскажающего линеаризатора (АПЛ)

Для упрощения вычислений квантователь уровня, корелятор и блок управления линеаризатором, алгоритм работы которого представлен на рис. 2, задавались программным методом с помощью соответствующих программных блоков Matlab встроенных в подпрограмму VSS.

На рис. 4 показана трехмерная поверхность процесса сходимости при переборе параметров линеаризатора p_1 и p_2 по критерию максимизации значения взаимно корреляционной функции.

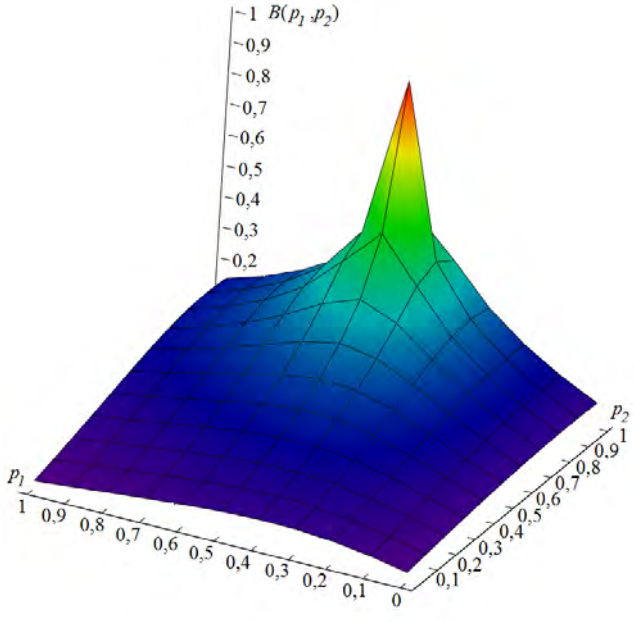

Рис. 4. Поверхность критерия качества $B(p_1, p_2)$ в процессе адаптации параметров линеаризатора

Результаты, представленные на рис. 4, показывают, что процесс двумерной адаптации параметров аналогового предыскажающего линеаризатора на основе разработанного алгоритма однозначен и приводит к восстановлению оптимальной настройки его нелинейных характеристик и снижению уровня интермодуляционных искажений на выходе усилителя мощности за несколько циклов адаптации.

Так же стоит отметить, что процесс оптимизации и подбора двух параметров линеаризатора (p_1, p_2) происходит одинаково, независимо от того, использовано аналоговое или цифровое устройство предыскажающей линеаризации [14–21].

Заключение

В данной работе предложено адаптивное устройство предыскажающей линеаризации, основанное на корреляционной оценке уровня нелинейных искажений на выходе усилителя мощности, позволяющее обеспечить более высокую эффективность линеаризации при меняющихся характеристиках бортового радиопередающего устройства в процессе длительного функционирования на борту космического аппарата. Еще одним существенным достоинством предложенного технического решения применительно к бортовой спутниковой аппаратуре являются более высокие показатели надежности и более простая техническая реализация по сравнению с аналогами, за счет отсутствия предварительной аналоговой и цифровой обработки СВЧ-сигнала. В статье показано, что процесс двумерной адаптации в блоке управления предыскажающим линеаризатором на основе разработанного алгоритма однозначен и приводит к восстановлению оптимальной настройки линеаризованного усилителя мощности и снижению уровня интермодуляционных искажений на его выходе за несколько циклов адаптации.

Литература

1. *Kenington P.B.* High-Linearity RF Amplifier Design. Artech House Inc., 2000. 552 p.

2. *CriPps S.C.* RF Power Amplifier for Wireless Communications. Artech House Inc, 1999. 472 p.

3. *Katz A., Sudarsanam R., Aubert C.* A reflective diode lineariser for spacecraft a Pplications // IEEE MTT-S Int. Microw. Symp. Dig., St. Louis, MO, USA, June 1985. Pp. 661–664.

4. *Roger F.* An Analog APproach to Power Amplifier Predistortion // Microwave Journal. 2011. Vol. 54. No. 4. Pp. 60–76.

5. *Villemazet J.F., Yahi H., Lefebvre B., Baudeigne F., Maynard J., Soubercaze-Pun G., Lapierreet L.* New Ka-Band Analog Predistortion Linearizer allowing a 2.9GHz Instantaneous Wideband Satellite Operation // 2017 47th European Microwave Conference (EuMC), 10–12 Oct. 2017. IEEE, 2017. Pp. 302–305.

6. *Воронецкий Е.В., Ксенофонтов С.М., Рожков В.М., Челноков О.А., Шестаков А.К.* Повышение эффективности усилителей многочастотных сигналов // Радиотехника. 1996. № 4. С. 73–79.

7. *Аверина Л.И., Бобрешов А.М., Шутов В.Д.* Адаптивный цифровой метод уменьшения внеполосного излучения усилителя мощности // Вестник Воронежского государственного университета.2013. № 1. С. 82–88.

8. *Zhou J., Zhai J., Liang X., Hong W.* An Automatic Error Compensation Method for the Feedback Loop in Adaptive DPD Systems // Microwave Journal. 2008. Vol. 51. No. 8. Pp. 64–83.

9. *Swaminathan J.N., Kumar P.* Design of Efficient Adaptive Predistorter for Nonlinear High Power Amplifier // Wireless Personal Comm. 2015. Vol. 82 (2). Pp. 1085–1093.

10. *Белов Л.А., Кондрашов А.С., Ромащенко К.В., Немаев М.А.* Адаптивная система линеаризации усилителей мощности широкополосных СВЧ-сигналов // Сб. докл. Междунар. науч.-техн. семин. «СИНХРОИНФО 2013», 30 июня–3 июля, Ярославль, 2013. С. 11–13.

11. *Белов Л.А., Кондрашов А.С., Петушков С.В.* Корреляционная оценка уровня интермодуляционных искажений СВЧ-сигналов в усилителях мощности // Электросвязь. 2015. № 5. С. 28–30.

12. *Petushkov S.V., Vilderman E.N., Belov L.A.* Influence of power amplifier's intermodulation distortion on transmitted information quality // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, Belarus, 4–5 July 2018. IEEE, 2018. Pp. 1–4. DOI: 10.1109/SYNCHROINFO.2018.8457049.

13. *Saleh A.* Frequency-independent and frequency–dependent nonlinear models of TWT amplifiers // IEEE Transactions on Communications. 1981. Vol. 29. Pp. 1715–1720.

14. *Феер К.* Беспроводная цифровая связь. Методы модуляции и расширения спектра: пер. с англ. М.: Радио и связь, 2000. 530 с.

15. *Mekechuk K., Kim W.J., Stapleton S.P.* Linearizing Power Amplifiers Using Digital Predistortion, EDA Tools and Test Hardware, High Frequency Electronics // High Frequency Electronics. 2004. Pp. 18–28.

16. *Aleiner B.* Digital Feed-Forward linearization // Microwave Journal. 2009. Vol. 52. No. 10. Pp. 110–120.

17. *Briffa M.A., Faulkner M.* Dynamically Biased Cartesian Feedback Linearization // Proceedings of the 43rd IEEE Vehicular Technology Conference, Secaucus, USA, VTC-93. 1993. Pp. 672–675.

18. *Соловьёва Е.Б.* Каскадный предкомпенсатор для линеаризации характеристик усилителя мощности // Цифровая обработка сигналов. 2013. № 1. С. 9–13.

19. *Солнцев В.А., Шульга А.И.* Анализ подавления нелинейных искажений в усилителях сигналом огибающей // Радиотехника и электроника. 2012. Т. 57. № 2. С. 219–229.

20. Патент РФ 2623807 RU Цифровое устройство предыскажения радиосигналов четными гармониками / Кондрашов А.С., Петушков С.В. Заявл. 09.06.2016; опубл. 29.06.2017, Бюл. № 19.

21. *Петушков С.В., Белов Л.А., Кондрашов А.С.* Использование чётных гармоник для цифрового предыскажения входного сигнала при линеаризации амплитудных характеристик СВЧ-усилителя мощности // T-Comm — Телекоммуникации и транспорт. 2016. Т. 10. № 6. С. 3–7.

ADAPTIVE PREDISTORTION DEVICE OF THE SATELLITE TRANSMITTERS

SERGEY V. PETUSHKOV

Moscow, Russia, petushkov.sv@spacecorp.ru

KEYWORDS: transmitter; power amplifier; intermodulation distortion; adaptive predistortion; predistortion linearization; correlation function.

ABSTRACT

The improvement of energetic and spectral characteristics of the satellite transmitters which act in the harsh space environment with the help of the predistortion linearization becomes more and more actual task. The proposed adaptive predistortion device is based on the correlation evaluation of the nonlinear distortion level at the output of the power amplifier. The device allows to provide more effective linearization in the conditions with changing characteristics of the satellite transmitter within the lifetime of the satellite at the orbit in difference to the systems with advance tuning. The proposed technical solution has a higher reliability and simplified technical implementation in comparison with the analogs due to lack of the preliminary analog and digital processing of the RF signal. The simplified algorithm which requires lesser logical capacity in the digital microcircuits than conventional adaptive algorithms was developed for the modeling of the adaptive predistortion device. The proposed algorithm of changing the parameters of the predistortion linearizer requires less mathematical calculations within one iteration cycle, which is based on the determination of the cross-correlation function gradient rise direction. The obtained results of proposed predistortion linearizer modeling show that the process of two-dimension adaptation based on the developed algorithm is monosemantic and leads to the recovery of the linearizer's non-linear characteristics optimal tune. The adaptation process leads to the lowering of the intermodulation distortion at the output of the power amplifier in a few adaptation cycles. It is worth noting that the process of the optimization and selection of the two parameters of the predistortion linearizer in the amplifier flows the same way whatever if the analog of digital implementation of the linearizer is used.

REFERENCES

1. Kenington P.B. *High-Linearity RF Amplifier Design.* Artech House Inc., 2000. 552 p.

2. CriPps S.C. *RF Power Amplifier for Wireless Communications*. Artech House Inc, 1999. 472 p.

3. Katz A., Sudarsanam R., Aubert C. A reflective diode lineariser for spacecraft a Pplications. *IEEE MTT-S Int. Microw. Symp. Dig., St. Louis,*

MO, USA, June 1985. Pp. 661–664.
4. Roger F. An Analog APproach to Power Amplifier Predistortion. *Microwave Journal*. 2011. Vol. 54. No. 4. Pp. 60–76.
5. Villemazet J.F., Yahi H., Lefebvre B., Baudeigne F., Maynard J., Soubercaze-Pun G., Lapierreet L. New Ka-Band Analog Predistortion Linearizer allowing a 2.9GHz Instantaneous Wideband Satellite Operation. *2017 47th European Microwave Conference (EuMC), 10–12 Oct. 2017*. IEEE, 2017. Pp. 302–305. DOI: 10.23919/EuMC.2017.8231024.
6. Voronetsky E.V., Ksenofontov S.M., Rozhkov V.M., Chelnokov O.A., Shestakov A.K. Increasing the efficiency of amplifiers of multifrequency signals. *Radiotekhnika*. 1996. No 4. Pp. 73–79.
7. Averina L.I., Bobreshov A.M., Shutov V.D. An adaptive digital method for reducing out-of-band radiation of a power amplifier. *Bulletin of Voronezh State University*. 2013, No. 1. Pp. 82–88.
8. Zhou J., Zhai J., Liang X., Hong W. An Automatic Error Compensation Method for the Feedback Loop in Adaptive DPD Systems. *Microwave Journal*. 2008. Vol. 51. No. 8. Pp. 64–83.
9. Swaminathan J.N., Kumar P. Design of Efficient Adaptive Predistorter for Nonlinear High Power Amplifier. *Wireless Personal Comm*. 2015. Vol. 82 (2). Pp. 1085–1093.
10. Belov L.A., Kondrashov A.S., Romashchenko K.V., Nemaev M.A. Adaptive system of linearization of power amplifiers of broadband microwave signals. *Coll. report Int. scientific and technical semin. SINCHROINFO 2013,* June 30 – July 3, Yaroslavl, 2013. Pp. 11–13.
11. Belov L.A., Kondrashov A.S., Petushkov S.V. Correlation estimation of the level of intermodulation distortion of microwave signals in power amplifiers. *Electrosvyaz*. 2015. No.5. Pp. 28–30.
12. Petushkov S.V., Vilderman E.N., Belov L.A. Influence of power amplifier's intermodulation distortion on transmitted information quality. *2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO),* Minsk, Belarus, 4–5 July 2018. IEEE, 2018. Pp. 1–4. DOI: 10.1109/SYNCHROINFO.2018.8457049.
13. Saleh A. Frequency-independent and frequency-dependent nonlinear models of TWT amplifiers. *IEEE Transactions on Communications*. 1981. Vol. 29. Pp. 1715–1720.
14. Feher K. *Wireless Digital Communications: Modulation and Spread Spectrum Applications*. Prentice Hall PTR, 1995. 544 p.
15. Mekechuk K., Kim W.J., Stapleton S.P. Linearizing Power Amplifiers Using Digital Predistortion, EDA Tools and Test Hardware, High Frequency Electronics. *High Frequency Electronics*. 2004. Pp. 18–28.
16.Aleiner B. Digital Feed-Forward linearization. *Microwave Journal*. 2009. Vol. 52. No. 10. Pp. 110–120.
17. Briffa M.A., Faulkner M. Dynamically Biased Cartesian Feedback Linearization. *Proceedings of the 43rd IEEE Vehicular Technology Conference, Secaucus, USA,* VTC – 93, May 1993. Pp. 672–675.
18. Solovyova E.B. Cascade precompensator for linearization of the characteristics of the power amplifier. *Cifrovaia obrabotka signalov.* 2013. No. 1. Pp. 9–13.
19. Solntsev V.A., Shulga A.I. Analysis of the suppression of nonlinear distortions in amplifiers with an envelope signal. *Radiotekhnika i electronica*. 2012. Vol. 57. No. 2. Pp. 219–229.
20. Patent № 2623807 RU. Digital predistortion of radio signals with even harmonics / Kondrashov A.S., Petushkov S.V. Decler 06.09.2016; publ. 06.29.2017. Bull. No. 19.

INFORMATION ABOUT AUTHOR:

Petushkov S.V., PhD, assistant of department "Generation and processing radio signals" NRU "MPEI", advanced engineer of JSC "Russian Space Systems".

For citation: Petushkov S.V. Adaptive predistortion device of the satellite transmitters. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 11–17. doi: 10.36724/2409-5419-2020-12-6-11-17 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-18-25

ОПТИМИЗАЦИЯ ПРОФИЛАКТИЧЕСКИХ ДОПУСКОВ В СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМАХ

АБРАМКИН
Роман Викторович[1]

ВИНОГРАДЕНКО
Алексей Михайлович[2]

СЛЕПОВ
Сергей Николаевич[3]

ДРОСС
Виталий Александрович[4]

АННОТАЦИЯ

В настоящее время контроль технического состояния сложных технических систем, таких как, электротехническое оборудование техники связи, представляет собой длительный и неавтоматизированный процесс, который осуществляются операторами непосредственно на самих объектах контроля. Данное обстоятельство оказывает негативное влияние на своевременность выявления отказов контролируемого объекта. Одним из наиболее сложно выявляемых является постепенный отказ. Для своевременного обнаружения факта его наступления необходимо создание системы контроля, работающей в перманентом режиме с заранее введенными профилактическими допусками. **Цель работы** заключается в разработке предложения по формированию оптимального значения профилактического допуска контролируемого параметра для обнаружения факта наступления постепенного отказа и определение его вероятностных характеристик с учетом резервирования измерительных каналов. **Используемые методы:** обнаружение постепенных отказов носит случайный характер и наилучшие результаты при этом получаются с использованием методов теории статистических решений, применение которых предполагает наличие полных априорных сведений о вероятностных распределениях выходных значений контролируемых параметров. **Новизна работы** заключается в повышении достоверности, точности контроля технического состояния сложных технических объектов для обеспечения их надежности путем резервирования измерительных каналов, что позволяет, повысить точность выявления постепенного отказа контролируемого объекта за счет оптимизации значения профилактических допусков. **Результат:** применение экономичного резервирования измерительных каналов, а также использование профилактических допусков позволяет более точно проводить оценку технического состояния объектаконтроля и делать вывод о вероятности наступления постепенного отказа. Оптимизация порога профилактического допуска позволяет минимизировать вероятность принятия ошибочного решения. **Практическая значимость:** результаты работы можно использовать в процессе контроля технического состояния сложных технических систем, что позволит избежать аварийных ситуаций.

КЛЮЧЕВЫЕ СЛОВА: контроль технического состояния; профилактический допуск; измерительный канал; резервирование; точность измерений; постепенный отказ; достоверность контроля; вероятность верного решения; вероятность ошибочного решения.

Сведения об авторах:

[1]адъюнкт Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, avg62rus@rambler.ru

[2]к.т.н., доцент, старший преподаватель Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, vinogradenko.a@inbox.ru

[3]к.т.н., доцент, старший научный сотрудник 16-го Центрального научно-исследовательского испытательного ордена Красной Звезды института имени маршала войск связи А. И. Белова Минобороны России, г. Мытищи, Россия, slepov69@yandex.ru

[4]к.т.н., доцент Военной академии связи им. Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, dross_vit@mail.ru

Для цитирования: *Абрамкин Р.В., Виноградено А.М., Слепов С.Н., Дросс В.А.* Оптимизация профилактических допусков в сложных технических системах // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 18–25. doi: 10.36724/2409-5419-2020-12-6-18-25

Введение

В настоящее время существующие системы контроля технического состояния не способны с необходимым качеством и заданной точностью выполнить всю полноту возлагаемых на них задач. Нынешняя оперативность проведения измерений и доставки информации лицу, принимающему решения, зачастую, оказывается гораздо ниже желаемой. На текущий момент, большинство операций контроля не автоматизированы, осуществляются операторами непосредственно на самих объектах контроля. Совокупность данных факторов оказывает крайне негативное влияние на своевременность выявления отказов объекта контроля. Одним из наиболее сложно выявляемых является постепенный отказ. Для его определения необходима система контроля, работа которой осуществляется непрерывно в режиме реального времени с целью перманентного обновления результата измерений. С целью повышения достоверности, надежности и точности измерений, необходимо резервировать измерительные каналы, что позволит ввести профилактические допуски для более эффективного выявления и предупреждения постепенных отказов контролируемого объекта. Резервирование измерительных каналов необходимо осуществлять там, где это действительно нужно, а именно в наиболее ответственных, особо важных элементах и узлах объекта контроля. Однако, жесткие требования по эргономике и массогабаритным показателям, предъявляемые к оборудованию аппаратных, не всегда позволяют наращивать число резервных каналов для достижения требуемого уровня непрерывности и достоверности измерений. Поэтому, в таких системах применятся минимальное число дублирующих каналов. Также, увеличение числа измерительных каналов оказывает существенное негативное влияние на канальный ресурс системы контроля технического состояния [1–2].

Резервирование измерительных каналов необходимо для повышения точности измерений, с целью использования профилактических допусков и повышения достоверности контроля технического состояния. В данном случае наиболее целесообразным будем считать применение предельного случая экономичного резервирования — двухканальной схемы резервирования, при которой резервируется один дублирующий канал.

Таким образом, основной задачей является повышение надежности, достоверности, точности контроля объектов путем корректировки работы измерительных каналов (их резервирование). Для реализации процедуры обнаружения факта отказа объекта контроля должен быть определен пороговый уровень (профилактический допуск) обнаружения отказа с учетом характера его влияния на вероятности принятия правильных и ошибочных решений о состоянии объекта контроля. Профилактический допуск представляет собой предельное значение параметра, при котором изделие считается еще работоспособным (не отказавшим), но подлежащим замене (регулировке) с целью предупреждения отказа [3–5].

Цель статьи — разработка предложения по формированию оптимального значения профилактического допуска контролируемого параметра для обнаружения факта наступления постепенного отказа и определение его вероятностных характеристик с учетом экономичного резервирования измерительных каналов.

Методы регистрации постепенных отказов

Выявление постепенных отказов представляет собой задачу определения вероятностных характеристик первопрохождения одномерным или векторным случайным процессом, отрезок реализации которого известен, определенного уровня или поверхности, ограничивающих область допустимых значений этого процесса.

Выявление постепенных отказов путем математического моделирования заключается в определении вероятностных свойств апостериорных случайных процессов изменения параметров, т.е. процессов, являющихся продолжениями отрезков реализаций, полученных путем индивидуального контроля, моделирования этих процессов и фиксации моментов выхода моделей процессов за пределы допустимых значений. Основной трудностью таковго метода является определение вероятностных свойств апостериорных процессов, а также в отыскании уравнений связи параметров элементов и выходных параметров устройства.

Выявление постепенных отказов методами распознавания образов состоит из двух этапов; обучения (классификации) и распознавания.

На этапе обучения реализации векторного случайного процесса изменения параметров разбиваются на классы по времени нахождения процесса в области допустимых значений. На основе достаточного количества реализаций процесса определяются вероятности каждого класса и по начальным отрезкам реализации условная вероятность попадания их в тот или иной класс. Определение вероятности каждого класса, по существу, представляет собой прогнозирование работоспособности для совокупности подобных устройств. На этапе распознавания анализируются начальный участок реализации векторного случайного процесса изменения параметров устройства и условная вероятность попадания этой реализации в каждый из классов. Эти условные вероятности и представляют собой распределение времени безотказной работы индивидуального устройства. Метод распознавания образов получил развитие для устройств, описываемых одним или двумя параметрами. Точность метода определяется количеством реализаций, используемых для обучения. При одной и той же точности необходимое количество реализаций возрас-

тает примерно пропорционально квадрату от числа параметров. Поэтому использование данного метода возможно после законченного цикла эксплуатации большого числа устройств [6–7].

Выявление постепенных отказов при помощи специальных испытаний заключается в физическом моделировании влияния основных возмущающих факторов, построении поверхности, ограничивающей область допустимых отклонений возмущающих факторов, и оценки запаса работоспособности. Для этого необходимо:

1) выявить основные возмущающие факторы;

2) создать искусственные условия, в которых эти факторы могут регулироваться;

3) провести испытания и рассчитать момент наступления постепенного отказа.

Данный метод является одним из наиболее ресурсозатратных.

В настоящее время для обнаружения отказов в контролируемых объектах используется интервальный метод, суть которого состоит в задании допустимого интервала значений выходной величины каждого контролируемого параметра (рабочего диапазона). При выходе этой величины за пределы рабочего диапазона принимается решение об отказе контролируемого элемента. Однако, данный метод является наиболее эффективным для выявления внезапных отказов. Процесс их обнаружения носит детерминированный характер.

Интервальный метод позволяет обнаруживать данные отказы с единичной вероятностью [8–10]. В нашем случае обнаружение постепенных отказов носит случайный характер и наилучшие результаты при этом получаются с использованием методов теории статистических решений, применение которых предполагает наличие полных априорных сведений о вероятностных распределениях выходных значений контролируемых параметров.

Основной причиной постепенных отказов является старение материалов и износ отдельных частей элементов. Они возникают вследствие теплового, вибрационного старения изоляции трансформаторов, генераторов, кабельных линий, коррозии металлических частей проводов, опор, оболочек кабелей, износа дугогасительных устройств коммутационных аппаратов при отключении токов короткого замыкания, вследствие деформации материалов и диффузии одного материала в другой. По мере эксплуатации электротехнических изделий в изоляции происходят сложные физико-химические процессы старения. Изоляция становится хрупкой, ломкой, появляются трещины, в результате чего уменьшается ее электрическая прочность, и при случайном превышении напряжения сверх допустимого значения происходит отказ. Аналогичные ситуации наблюдаются при коррозии и окислении металлических частей элементов и при воздействии механических нагрузок (постепенное снижение прочности и в случае превышения запаса прочности — отказ). Таким образом, постепенный износ отдельных частей элемента представляет собой накопление элементарных повреждений в различных его частях и снижение общего предела прочности. После накопления определенного числа элементарных повреждений происходит отказ элемента. Для наступления постепенного отказа необходимо многократное превышение допустимого параметра, например, температуры изоляции сверх допустимого значения, либо многократное отключение выключателем токов коротких замыканий. Для построения математического описания этих явлений используют простейший поток событий — в случайные моменты времени происходят единичные элементарные повреждения и при их накоплении объект отказывает.

Использованием методов теории статистических решений является наиболее подходящим вариантом данном случае, так как предполагает наличие полных априорных сведений о вероятностных распределениях выходных значений контролируемых параметров (границы работоспособного состояния известны и определены руководящими документами на изделия) [11–13].

Рассмотрим объект контроля технического состояния, в котором производится непрерывное измерение значения контролируемого параметра. Будем считать, что получаемые значения являются случайными величинами X (предшествующее измеренное значение) и Y (текущее измеренное значение) и характеризуются одинаковыми вероятностными распределениями с параметрами: $M[X] = M[Y] = m$; $M[(X-m)^2] = M[(Y-m)^2] = \sigma^2$. Для значений X и Y определим диапазон всех физически возможных значений β и диапазон работоспособности α. Диапазон α располагается внутри диапазона β ($\alpha < \beta$) и разделяет его на три части: A_1 — соответствует диапазону работоспособности α, A_2 — расположена ниже диапазона α, A_2 — расположена выше диапазона α.

Обнаружение факта наступления отказа осуществляется в соответствии с условием

$\Delta > \Delta^*$ — отказ объекта контроля,

$\Delta \le \Delta^*$ — объект контроля исправен, (1)

где $\Delta = |Y - \%|$, $\varnothing^*$ — пороговый уровень обнаружения отказа (профилактический допуск), $\Delta^* \le \alpha$.

Вероятностные характеристики объекта контроля, функционирующего в условиях постепенных отказов

Принятие решения об отказе контролируемого объекта в соответствии с условием (1) носит вероятностный характер. При этом возможны следующие варианты, составляющие полную группу несовместных событий:

1) выходные значения X и Y находятся в диапазоне значений A_1 (отказа нет), а модуль их разности $\varnothing$ не пре-

высил порог $\varnothing^*$ (правильное решение об исправности объекта);

2) выходные значения X и Y находятся в диапазоне значений A_2 (отказа нет), а модуль их разности $\varnothing$ превысил порог (ложное решение об отказе объекта);

3) одно или оба значения X, Y находятся в диапазоне значений A_2 или A_3, а модуль разности сигналов $\varnothing$ превысил порог (правильное решение об отказе объекта);

4) один или оба сигнала X и Y находятся в диапазоне значений A_2 или A_3, а модуль разности сигналов $\varnothing$ не превысил порог (ложное решение об исправности объекта) [15].

Варианты состояний контролируемого объекта с возможными исходами процедуры обнаружения отказа представлены на рис. 1, где приняты следующие обозначения: НС — начальное состояние объекта; Отк — отказ объекта; Исп — исправность объекта; ВРО — верное решение об отказе объекта; ОРИ — ошибочное решение об исправности объекта; ВРИ — верное решение об исправности объекта; ОРО — ошибочное решение об отказе объекта; $P_{отк}$ — вероятность отказа объекта; $P_{исп}$ — вероятность исправности объекта; $P_{ппотк}$ — вероятность превышения порога в случае отказа объекта; $P_{нпотк}$ — вероятность непревышения порога в случае отказа объекта; $P_{пписп}$ — вероятность превышения порога в случае исправности объекта; $P_{нписп}$ — вероятность непревышения порога в случае исправности объекта; $P_{вроо}$ — вероятность верного решения об отказе объекта; $P_{орио}$ — вероятность ошибочного решения об исправности объекта; $P_{врио}$ — вероятность верного решения об исправности объекта; $P_{ороо}$ — вероятность ошибочного решения об отказе объекта[1].

Введем описание исправного $S_{исп}$ и неисправных состояний объекта контроля $S_{отк}(i,j)$:

$$\begin{aligned} S_{исп} &= X \in A_1 \wedge Y \in A_1, \\ S_{отк}(i,j) &= X \in A_i \wedge Y \in A_j, \\ i, j &= \overline{1,3}. \end{aligned} \tag{2}$$

Причем $S_{отк}(1,1) = \varnothing$, так как этот случай соответствует исправному состоянию $S_{исп}$.

Вероятности введенных состояний определяются следующими выражениями:

$$\begin{aligned} P_{исп} &= \int_{A_1} w_X(X) \cdot \int_{A_1} w_Y(Y) dY dX, \\ P_{отк} &= \int_{A_i} w_X(X) \cdot \int_{A_j} w_Y(Y) dY dX, \\ i, j &= \overline{1,3}, \end{aligned} \tag{3}$$

где $w_X(X)$, $w_Y(Y)$ — плотности вероятности случайных величин X и Y.

В случае исправного объекта контроля (состояние $S_{исп}$) возможно верное решение о его исправности или ошибочное решение о его отказе, вероятности которых определяются как:

$$\begin{aligned} P_{врис} &= P_{исп} \cdot P_{нписп}, \\ P_{орос} &= P_{исп} \cdot P_{пписп}, \end{aligned} \tag{4}$$

где $P_{исп}$ и $P_{нписп}$ — вероятности превышения и непревышения величиной $\varnothing$ порога $\varnothing^*$ в случае исправности объекта;

[1]Фомин Л.А. Черноскутов А.И. Оптимизация ошибок при двухэтапной процедуре контроля // Автоматика и вычислительная техника. 1975. № 3. С. 34-37.

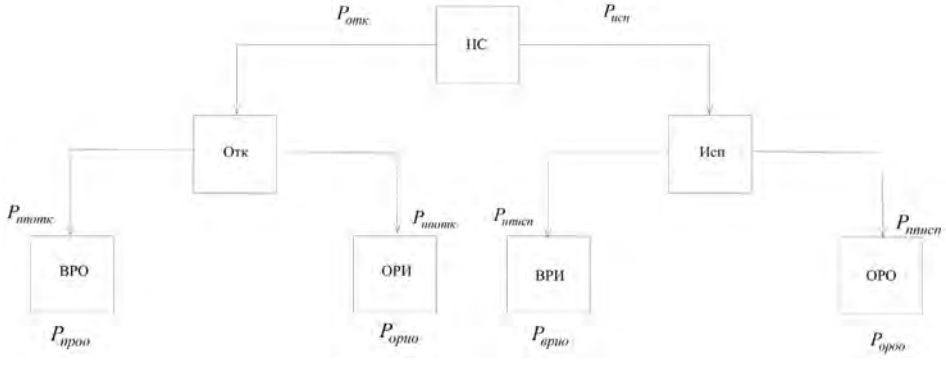

Рис. 1. Варианты состояний объекта контроля

$$P_{\text{нписп}} = \int_0^{\Delta^*} w_\Delta(\Delta / A_1, A_1) d\Delta,$$

$$P_{\text{пписп}} = \int_{\Delta^*}^{\alpha} w_\Delta(\Delta / A_1, A_1) d\Delta, \quad (5)$$

где $w_\varnothing(\varnothing / A_1, A_1)$ — условная плотность вероятности величины $\varnothing$ при попадании X и Y в диапазон значений A_1.

В случае неисправности объекта контроля (состояния $S_{\text{отк}}(i,j)$, $i, j = \overline{1,3}$) возможны верные решения о его отказе или ошибочные решения о его исправности, вероятности которых определяются как:

$$P_{\text{вроо}}(i,j) = P_{\text{отк}}(i,j) \cdot P_{\text{ппотк}}(i,j),$$
$$P_{\text{орио}}(i,j) = P_{\text{отк}}(i,j) \cdot P_{\text{нпотк}}(i,j), \quad (6)$$
$$i, j = \overline{1,3}$$

где $P_{\text{ппотк}}(i,j)$ и $P_{\text{нпотк}}(i,j)$ вероятности превышения и непревышения величиной $\varnothing$ порога $\varnothing^*$ в случае отказа объекта;

$$P_{\text{ппотк}}(i,j) = \int_{\Delta^*}^{\Delta_{\max}(i,j)} w_\Delta(\Delta / A_i, A_j) d\Delta, \quad (7)$$

$$P_{\text{нпотк}}(i,j) = \int_{\Delta_{\min}(i,j)}^{\Delta^*} w_\Delta(\Delta / A_i, A_j) d\Delta,$$
$$i, j = \overline{1,3}$$

где $w_\varnothing(\varnothing / A_i, A_j)$ — условная плотность вероятности величины $\varnothing$ при попадании X и Y в диапазон значений A_i и A_j соответственно, а $\varnothing_{\min}(i,j)$ и $\varnothing_{\max}(i,j)$ — минимальные и максимальные значения величины $\varnothing$ в ситуации $S_{\text{отк}}$, с учетом всех состояний отказа объекта получаем вероятности верного решения об отказе $P_{\text{вроо}}$ и ошибочного решения об исправности $P_{\text{орио}}$:

$$P_{\text{вроо}} = \sum_{i=1}^{3} \sum_{j=1}^{3} P_{\text{вроо}}(i,j),$$
$$P_{\text{орио}} = \sum_{i=1}^{3} \sum_{j=1}^{3} P_{\text{орио}}(i,j). \quad (8)$$

Исходы, соответствующие верным и ошибочным решениям о состоянии объекта, могут быть объединены в благоприятный и неблагоприятный исходы с соответствующими вероятностями верного и ошибочного решений:

$$P_{\text{ВР}} = P_{\text{врио}} + P_{\text{вроо}},$$
$$P_{\text{ОР}} = P_{\text{орио}} + P_{\text{ороо}}. \quad (9)$$

Поскольку благоприятные и неблагоприятные исходы являются противоположными событиями, то сумма их равна единице:

$$P_{\text{ВР}} + P_{\text{ОР}} = 1 \quad (10)$$

Выбор порога $\varnothing^*$ следует осуществлять путем решения задачи ошибок первого и второго рода, то есть оптимизацией $P_{\text{ОР}}$ и $P_{\text{ВР}}$ для конкретного объекта контроля:

$$\Delta^*_{opt} = Arg \max_{\Delta^* \in [0;\alpha]} P_{\text{ВР}}(\Delta^*) = Arg \min_{\Delta^* \in [0;\alpha]} P_{\text{ОР}}(\Delta^*).$$

Оптимизация профилактических допусков

Возможен случай, при котором случайные величины X и Y распределены по равномерному закону в диапазоне возможных значений β, причем зона α расположена симметрично относительно математических ожиданий X и Y [14]. При этом значения β определяются исходя из заданной вероятности безотказной работы объекта контроля $P_{\text{ок}}$ в соответствии с выражением $P_{\text{ок}} = \frac{\alpha}{\beta}$, что обусловлено равномерным законом распределения X и Y. Для определения конечных исходов необходимо знать условные плотности распределения вероятностей $w_\varnothing(\varnothing / A_i, A_j)$ $i, j = \overline{1,3}$, вычисление которых было произведено в [15]. Тогда на основании расчетов с использованием выражений (3)–(8) аналитические выражения для вероятностей конечных исходов примут вид:

$$P_{\text{прио}} = \begin{cases} \dfrac{2\alpha\Delta^* - \Delta^{*2}}{\beta^2}, & 0 < \Delta^* < \alpha, \\ \dfrac{\alpha^2}{\beta^2}, & \Delta^* = \alpha \end{cases} \quad (11)$$

$$P_{\text{лроо}} = \begin{cases} \dfrac{\alpha^2 - 2\alpha\Delta^* + \Delta^{*2}}{\beta^2}, & 0 < \Delta^* < \alpha, \\ 0, & \Delta^* = \alpha \end{cases}$$

$$P_{\text{проо}} = \frac{\beta^2 - \alpha^2 - 2\beta\Delta^* + 2\alpha\Delta^*}{\beta^2}, \quad 0 < \Delta^* < \alpha \quad (12)$$

$$P_{\text{лрио}} = \frac{2\beta\Delta^* - 2\alpha\Delta^*}{\beta^2}, \quad 0 < \Delta^* < \alpha$$

Исходя из расчетов, представленных в [15], можно сделать вывод, что существует оптимальное значение профилактического допуска $\Delta^* = \Delta^*_{opt}$, которому соответствует максимальное значение вероятности верных решений и минимальное значение ошибочных решений. При этом значения зависят от соотношения $\frac{\alpha}{\beta}$:

$$\Delta^*_{opt} = Arg \max_{\Delta^* \in [0;\alpha]} P_{\text{ВР}}(\Delta^*, \frac{\alpha}{\beta}) = Arg \min_{\Delta^* \in [0;\alpha]} P_{\text{ОР}}(\Delta^*, \frac{\alpha}{\beta}) \quad (13)$$

Заключение

Отсутствие автоматизированного контроля технического состояния, и, соответственно, возможности выявления и предупреждения постепенных отказов отрицательно сказывается на эффективности функционирования контролируемого объекта.

Применение экономичного резервирования измерительных каналов, а также использование профилактических допусков (порогов) позволяет более точно проводить оценку технического состояния объекта контроля и делать вывод о вероятности наступления постепенного отказа.

При выборе порога $\varnothing^*$, его необходимо оптимизировать таким образом, чтобы минимизировать вероятность принятия ошибочного решения (об отказе и исправности). Выбор профилактического допуска $\varnothing^*$ необходимо производить с учетом отношения диапазона работоспособности к диапазону всех физически возможных значений параметра, что обеспечит максимум вероятности верных решений о состоянии объекта контроля.

Литература

1. *Абрамов О.В.* Функционально-параметрическое направление теории рисков: возможности и перспективы // Вестник ДВО РАН: «Информатика и управление в технических системах». 2016. № 4. С. 96–101.

2. *Будко П.А., Виноградено А.М., Кузнецов С.В, Гойденко В.К.* Реализация метода многоуровневого комплексного контроля технического состояния морского робототехнического комплекса // Системы управления, связи и безопасности. 2017. № 4. С. 71–101.

3. *Мальцев Г.Н., Якимов В.Л.* Достоверность многоэтапного контроля технического состояния объектов испытаний // Информационно-управляющие системы. 2018. № 1. С. 49–57.

4. *Виноградено А.М.* Прогнозирование отказов контролируемых комплексов связи специального назначения // Системы управления, связи и безопасности. 2020. № 3. С. 222–237.

5. *Клячкин В.Н., Карпунина И.Н., Федорова М.К.* Оценка стабильности температурного режима компьютера // Автоматизация процессов управления. 2016. № 3 (45). С. 58–64.

6. *Климов В.В., Крапивин В.Ф., Мкртчян Ф.А., Ничипор А.Е.* Методы классификации и качественной интерпретации данных дистанционного мониторинга окружающей среды // Экологические системы и приборы. 2002. № 3. С. 7–12.

7. *Кузьмин А.Б.* Функциональное диагностирование технической системы управления // Автоматика и телемеханика. 1994. № 5. С. 183–189.

8. *Михайлов Р.Л., Макаренко С.И.* Оценка устойчивости сети связи в условиях воздействия на нее дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4. С. 69–79.

9. *Федоренко В.В., Федоренко И.В.* Модель формирования сигнала тревоги в интегрированной ТМС // Автоматизация, телемеханизация и связь в нефтяной промышленности. 2013. № 11. С. 41–45.

10. *Антонюк Е.М., Ломоносова Ю.С.* Системы автоматического контроля со сжатием данных // Известия СПбГЭТУ (ЛЭТИ). 2009. № 7. С. 62–68.

11. *Акуленко Л.Д., А.М. Шматков* Оптимальное по быстродействию приведение динамического объекта на поверхность эллипсоида в многомерном пространстве // Доклады Академии наук. 2017. Т. 477. № 1. С. 29–33.

12. *Буков В.Н., Максименко И.М.* Три подхода к задаче контроля технического состояния // Автоматика и телемеханика. 1995. № 3. С. 165–178.

13. *Бурый А.С., Лобан А.В., Ловцов Д.А* Модели сжатия массивов измерительной информации в автоматизированной системе управления // Автоматика и телемеханика. 1998. № 5. С. 3–26.

14. *Волобуев М.Ф., Уфаев В.А.* Обнаружение постепенных отказов в резервированной измерительной системе в зависимости от полноты вероятностного описания выходных сигналов // Информационно-измерительные и управляющие системы. 2017. Т. 15. № 10. С. 28–35.

15. *Волобуев М.Ф., Мальцев А.М., Михайленко С.Б., Уфаев В.А.* Способ обнаружения отказов при экономичном резервировании бортового оборудования беспилотного летательного аппарата // Журнал Сибирского федерального университета. Техника и технологии. 2016. № 9 (7). С. 1060–1067.

DETECTION OF GRADUAL FAILURES TAKING INTO ACCOUNT PREVENTIVE TOLERANCES AND COST-EFFECTIVE REDUNDANCY OF MEASUREMENT CHANNELS

ROMAN V. ABRAMKIN
St. Petersburg, Russia, avg62rus@rambler.ru

ALEXEY M. VINOGRADENKO
St. Petersburg, Russia, vinogradenko.a@inbox.ru

SERGEI N. SLEPOV
Mytishchi, Russia, slepov69@yandex.ru

VITALY A. DROSS
St. Petersburg, Russia, dross_vit@mail.ru

KEYWORDS:technical condition monitoring; preventive admission; measurement channel; redundancy; measurement accuracy; gradual failure; reliability of control; probability of a correct decision; probability of a wrong decision.

ABSTRACT

Currently, monitoring the technical condition of complex technical systems, such as electrical equipment of communication equipment, is a long and non-automated process that is carried out by operators directly at the control objects themselves. This circumstance has a negative impact on the timely detection of failures of the controlled object. One of the most difficult to detect is phasing out. For timely detection of the fact of its occurrence, it is necessary to create a control system that works in a permanent mode with pre-entered preventive tolerances. **The purpose of the work** is to develop a proposal for the formation of the optimal value of the preventive tolerance of the controlled parameter for detecting the fact of gradual failure and determining its probabilistic characteristics, taking into account the reservation of measurement channels. **Methods used**: detection of gradual failures is random and the best results are obtained using methods of statistical decision theory, the use of which assumes the presence of complete a priori information about the probability distributions of the output values of the controlled parameters. **The novelty of the work** is to increase the reliability and accuracy of monitoring the technical condition of complex technical objects to ensure their reliability by reserving measurement channels, which allows you to increase the accuracy of detecting gradual failure of the controlled object by optimizing the value of preventive tolerances. **Result:** the use of cost-effective redundancy of measurement channels, as well as the use of preventive tolerances, allows more accurate assessment of the technical condition of the control object and make a conclusion about the probability of gradual failure. Optimization of the threshold of preventive admission allows you to minimize the probability of making an erroneous decision. **Practical significance:** the results of the work can be used in the process of monitoring the technical condition of complex technical systems, which will avoid accidents.

REFERENCES

1. Abramov O.V. Functional nonparametric addition of risk theory: voter and prospects. *Vestnik DVO RAN: "Informatika i upravlenie v tekhnicheskih sistemah"* [Bulletin of the Feb RAS: "Informatics and administration in text systems"]. 2016. No. 4. Pp. 96–101. (In Rus)

2. Budko P.A., Vinogradenko A.M., Kuznecov S.V, Gojdenko V.K. Implementation of the method of multi-level integrated control of the technical condition of the marine robotic complex. *Sistemy upravleniya, svyazi i bezopasnosti* [Control systems, communications and security]. 2017. No. 4. Pp. 71–101. (In Rus)

3. Mal'cev G.N., YAkimov V.L. Dostovernost' mnogoetapnogo kontrolya tekhnicheskogo sostoyaniya ob"ektov ispytanij [Reliability of multi-stage control of the technical condition of test objects]. *Informacionno-upravlyayushchie sistemy* [Information and control systems]. 2018. No. 1. Pp. 49–57. (In Rus)

4. Vinogradenko A.M. Prognozirovanie otkazov kontroliruemyh kompleksov svyazi special'nogo naznacheniya [Forecasting failures of controlled communication complexes for special purposes]. *Sistemy upravleniya, svyazi i bezopasnosti* [Control systems, communications and security]. 2020. No. 3. Pp. 222–237. (In Rus)

5. Klyachkin, V.N., Karpunina I.N., Fedorova M.K Ocenka stabil'nosti temperaturnogo rezhima komp'yutera [Gime of a computer]. *Avtomatizaciya processov upravleniya* [Automation of control processes]. 2016. No. 3 (45). Pp. 58–64. (In Rus)

6. Klimov V.V., Krapivin V.F., Mkrtchyan F.A., Nichipor A.E. Methods of classification and qualitative interpretation of remote environmental Monitoring Data. *Ekologicheskie sistemy i pribory* [Environmental systems and devices]. 2002. No. 3. Pp. 7–12. (In Rus)

7. Kuz'min A.B. Functional diagnostics of the technical control system]. *Automation and Remote Control.* 1994. Vol. 55. No. 5. Pp. 765–769.

8. Mihajlov R.L., Makarenko S.I. Assessment of the stability of the communication network under the influence of destabilizing factors. *Radiotekhnicheskie i telekommunikacionnye sistemy* [Radio engineering and telecommunication systems]. 2013. No. 4. Pp. 69–79. (In Rus)
9. Fedorenko V.V., Fedorenko I.V. Model of alarm signal formation in integrated TMS. *Avtomatizaciya, telemekhanizaciya i svyaz' v neftyanoj promyshlennosti* [Automation, telemechanization and communication in the oil industry]. 2013. No. 11. Pp. 41–45. (In Rus)
10. Antonyuk E.M., Lomonosova YU.S. Sistemy avtomaticheskogo kontrolya so szhatiem dannyh [Automatic control systems with data compression]. *Izvestiya SPbGETU (LETI)* [Izvestiya SPbGETU (LETI)]. 2009. No. 7. Pp. 62–68. (In Rus)
11. Akulenko L.D., Shmatkov A.M. A time-optimal setting of a dynamic object on an ellipsoid surface in multidimensional space. *Doklady Physics*. 2017. Vol. 62. No. 11. Pp. 503–506.
12. Bukov V.N., Maksimenko I.M. Three approaches to the problem of technical condition control. *Automation and Remote Control*. 1995. Vol. 56. No. 3. Pp. 441–451.
13. Buryj A.S., Loban A.V., Lovcov D.A [Models of compression of measurement information arrays in an automated control system. *Automation and Remote Control*. 1998. Vol. 59. No. 5. Pp. 613–631.
14. Volobuev M.F., Ufaev V.A. Detection of gradual failures in a redundant measurement system depending on the completeness of the probabilistic description of output signals. *Informacionno-izmeritel'nye i upravlyayushchie sistemy* [Information-measuring and control systems]. 2017. Vol. 15. No. 10. Pp. 28–35. (In Rus)
15. Volobuev M.F., Mal'cev A.M., Mihajlenko S.B., Ufaev V.A. Method for detecting failures in the economical reservation of onboard equipment of an unmanned aerial vehicle. *Zhurnal Sibirskogo federal'nogo universiteta. Tekhnika i tekhnologii* [Journal of the Siberian Federal University. Equipment and technologies]. 2016. No. 9 (7). Pp. 1060–1067. (In Rus)

INFORMATION ABOUT AUTHORS:

Abramkin R.V. postgraduate student of the 42nd Department, military Academy of communications named after S. M. Budyonny;
Vinogradenko A.M. PhD, associate Professor, senior lecturer of the 42nd Department, military Academy of communications named after S. M. Budyonny;
Slepov S.N., PhD, associate Professor, senior researcher of the laboratory of 441 44 division 4 control, 16 Central research and testing Institute of the Russian Ministry of defense;
Dross V.A. PhD, associate Professor of the 42nd Department, military Academy of communications named after S. M. Budyonny.

For citation: Abramkin R.V., Vinogradenko A.M., Slepov S.N., Dross V.A. Detection of gradual failures taking into account preventive tolerances and cost-effective redundancy of measurement channels. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 18–25. doi: 10.36724/2409-5419-2020-12-6-18-25 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-26-37

ПРОГРАММНЫЙ КОМПЛЕКС МОДЕЛИРОВАНИЯ ПАКЕТНЫХ РАДИОСЕТЕЙ КВ-ДИАПАЗОНА

ДОРОГОВ
Александр Юрьевич[1]

ЯШИН
Александр Иванович[2]

АННОТАЦИЯ

В работе отмечено, что сложность и постоянная изменчивость структуры ионосферы, наличие множества факторов оказывающих влияние на распространения радиоволн в такой среде, а также сложная топология сетей связи приводят к необходимости компьютерного моделирования передачи данных в сетях КВ-диапазона. Описаны существующие модели представления ионосферных процессов и цифровых радиоканалов. Показано, что для решения задач проектирования радиосети передачи данных необходимо комплексное моделирования с учётом топологии сети, потерь распространения сигнала в радиоканале, уровня шума, вида цифровой модуляции, радиопрогноза условий связи. В работе рассмотрен моделирующий комплекс для пакетных радиосетей передачи данных КВ-диапазона с изменяющимися условиями связи. Комплекс состоит из совокупности взаимодействующих моделей реализованных в программной среде Matlab. Программная модель Прогнозирования условий связи соответствует рекомендации МСЭ-R P.533-13 Международного Союза Электросвязи (ITU). Приведено описание модели для режимов «Точка-точка» и «Зона» и показаны результаты её применения для расчёта протяжённых радиолиний. Описаны исходные данные и системные параметры модели. Представлена модель цифрового радиоканала КВ-диапазона. Для моделирования использован пакет Communications System Toolbox, входящий в состав программной среды Matlab. Описаны входные и выходные данные модели. Разработана модель Ионосферно-Волновой Частотно-Диспетчерской службы радиосети, предназначенная для построения волнового расписания устойчивой работы КВ-радиолиний сети. Описаны правила построения двухчастотного и многочастотного волнового расписания. Предложена схема моделирования процесса функционирования пакетной радиосети при изменяющихся условиях связи. Комплекс позволяет оценить вероятностно-временные характеристики радиолиний и зонового радио-покрытия в зависимости от географических координат, времени, месяца, солнечной активности и выбранных системных параметров на период до одного года. Приведены примеры использования моделирующего комплекса для расчёта протяжённых радиолиний сети КВ-диапазона. Целью данной работы является постановка задачи имитационного моделирования КВ-радиосетей при изменяющихся условиях связи.

КЛЮЧЕВЫЕ СЛОВА: ионосфера; радиолиния; цифровой модем; радиозона; радиосеть; применимые частоты; отношение сигнал/шум; волновое расписание.

Сведения об авторах:

1д.т.н., доцент, главный научный сотрудник ПАО «Информационные телекоммуникационные технологии («Интелтех»)», г. Санкт-Петербург, Россия, vaksa2006@yandex.ru

2д.т.н., профессор, Зам. Ген. Директора ПАО «Информационные телекоммуникационные технологии («Интелтех»)», г. Санкт-Петербург, Россия, vaksa2006@yandex.ru

Для цитирования: *Дорогов А.Ю., Яшин А.И.* Программный комплекс моделирования пакетных радиосетей КВ-диапазона // Наукоемкие технологии в космических исследованиях Земли. 2020.Т. 12. № 6. С. 26–37. doi: 10.36724/2409-5419-2020-12-6-26-37

Введение

Ионосферная радиосвязь в КВ диапазоне (3÷30 мГц) является экономически эффективной средой для многих видов телекоммуникационных услуг, требующих передачи данных за пределы прямой видимости. Для Российской Федерации высоконадёжная сеть КВ-диапазона масштаба страны представляется недорогой альтернативой спутниковым системам связи при предоставлении телекоммуникационных услуг службам МЧС, РЖД, силовым ведомствам, а также региональным администрациям и многочисленным хозяйственно-экономическим структурам.

Для КВ-диапазона определяющим фактором распространения радиоволн является наличие околоземной ионосферы. Структура и свойства ионосферы существенно изменяются с высотой. Процессы, протекающие в ионосфере, тесно связаны с волновым и корпускулярным излучением Солнца, с процессами в магнитосфере, вариациями магнитного поля Земли, с движением верхней атмосферы и т.д.[1] Этим обусловлена сильная изменчивость свойств ионосферы от времени суток, времени года, циклов солнечной активности, а также в зависимости от высоты и наличия отражающего слоя, географической широты и долготы приёмника и передатчика. Следующие физические явления КВ-диапазона, оказывают существенное влияние на построение системы передачи данных:

– нестационарная помеховая обстановка, вызванная изменяющимися условиями распространения радиоволн и работой сторонних систем радиосвязи;

– неселективные замирания длительностью 4…20 секунд;

– многолучевое распространение сигнала с временем многолучёвости до 5…6 мс., и доплеровским размытием между лучами до 2 Гц;

– сосредоточенные помехи в канале с уровнем до + 60 Дб от уровня сигнала.

Сложность и постоянная изменчивость структуры ионосферы, наличие множества факторов оказывающих влияние на распространения радиоволн в такой среде, а также сложная топология сетей связи приводят к необходимости компьютерного моделирования передачи данных в сетях КВ-диапазона. Длительную историческую традицию имеет подход, основанный на использовании ионосферных моделей, как правило, из класса статистических среди которых наиболее распространённой и обоснованной в настоящее время является модель IRI (International Reference Ionosphere[2]. IRI — это международный проект, спонсируемый Комитетом по космическим исследованиям (COSPAR) и Международным союзом радиовещания (URSI). Эти организации создали рабочую группу, которую вошли представители различных стран, в том числе и из России. Модель ионосферы впервые была предложена в конце 60-х на основе всех доступных источников данных. Выпущено несколько версий модели, в настоящее время действует модель IRI-2016. Для данного местоположения, времени и даты IRI предоставляет медианные значения электронной плотности, электронной температуры, температуры ионов, состава ионов в диапазоне ионосферных высот, критические частоты распространения радиоволн КВ-диапазона [1,2,3] и другие данные. Модель поддержана программными средствами открытого доступа, реализованными на языках Fortran, Python, Matlab [3,4]. К сожалению, модель не охватывает полностью спектр задач прогнозного моделирования распространения радиоволн на протяжённых трассах. В частности моделью не поддерживается расчёт уровней потерь на радиотрассах, влияние естественных и индустриальных помех на распространение сигнала, многолучевое распространение радиоволн, селективные замирания сигналов и другие характеристики, необходимые для проектирования КВ-радиосетей. Существует ряд рекомендательных моделей[3] разработанных Международным Союзом Электросвязи (ITU) дополняющих модель IRI. Вопросы моделирования радиолиний на основе данных рекомендаций рассматривались в работах [5,6,7,8,9].

В ITU разработана также комплексная математическая модель для прогнозирования рабочих характеристик ВЧ-линий, интегрирующая в себе набор частных моделей. Комплексная модель оформлена в виде рекомендации МСЭ-R P.533-13[3] и программных средств для ОС Windows на языке Fortran[5]. Модель позволяет производить расчёт характеристик КВ-радиолиний с протяжённостью до 9000 км (в режиме «Точка-точка») и радиозон покрытия (в режиме «Зона») с учётом уровней потерь на радиотрассах,

[1]Ионосфера и распространение радиоволн // ИЗМИРАН — институт земного магнетизма. URL: https://www.izmiran.ru/ionosphere/ (дата обращения: 23.06.2020).

[2]Международная справочная модель IRI // The International Reference Ionosphere. URL: http://irimodel.org/ (дата обращения: 23.06.2020).

[3]РЕКОМЕНДАЦИЯ МСЭ-R P.1623-1 Метод прогнозирования динамики замирания сигнала на трассах Земля-космос. URL: https://www.itu.int/pub/R-REC/ru.
РЕКОМЕНДАЦИЯ МСЭ-R P.368-9 Кривые распространения земной волны для частот между 10 кГц и 30 МГц. URL: https://www.itu.int/pub/R-REC/ru.
РЕКОМЕНДАЦИЯ МСЭ-R P.372-11 Радиошум. URL: https://www.itu.int/pub/R-REC/ru
РЕКОМЕНДАЦИЯ МСЭ-R P.1407-3 Многолучевое распространение и параметризация его характеристик. URL: https://www.itu.int/pub/R-REC/ru.
RECOMMENDATION ITU-R F.1487*, TESTING OF HF MODEMS WITH BANDWIDTHS OF UP TO ABOUT 12 kHz USING IONOSPHERIC CHANNEL SIMULATORS. URL: http://www.itu.int/pub/R-REC/en.
РЕКОМЕНДАЦИЯ МСЭ-R P.1240-2 Методы прогнозирования основной МПЧ, рабочей МПЧ и траектории луча, разработанные МСЭ-R. URL: https://www.itu.int/pub/R-REC/ru.

[4]РЕКОМЕНДАЦИЯ МСЭ-R P.533-13 (07/2015) Метод для прогнозирования рабочих характеристик ВЧ-линий. Серия P. Распространение радиоволн. . URL: https://www.itu.int/pub/R-REC/ru.

[5]REC533 Propagation Model // Institute for Telecommunication Sciences. URL: https://www.its.bldrdoc.gov/resources/radio-propagation-software/high-frequency/rec533-propagation-model.aspx (дата обращения: 23.06.2020).

влияние естественных и индустриальных помех на распространение сигнала, многолучевого распространение радиоволн. Программные средства доступны в виде исполняемых программ моделирующего комплекса и исходных кодов отдельных подпрограмм. В состав комплекса входит база данных антенн и редактор для изменения их характеристик. Комплексный характер модели позволяет минимизировать затраты на разработку дополнений.

Следует отметить, что исходные коды комплексной модели написаны на языке Fortran старой версии и поэтому требуют адаптации к современным компиляторам. Для отдельных подпрограмм представлен управляющий интерфейс, реализованный на основе устаревшей библиотеки ClearWin+. Исходные коды представляют собой набор подпрограмм и статических библиотек из программных модулей. Программный интерфейс к модулям не стандартизован. Указанные обстоятельства потребовали модификации исходного программного обеспечения и разработки собственного программного и пользовательского интерфейса для моделирующего комплекса. В новом варианте программный и пользовательский интерфейсы были реализованы средствами программной среды Matlab. Новый моделирующий комплекс использует структуру директориев исходного комплекса, и полностью совместим с ним по форматам хранения данных. Представленные модели дополняют разработанный ранее [1] комплекс имитационного моделирования сетевых и транспортных протоколов пакетной радиосети. В статье представлены принципы построения моделирующего комплекса на основе комплексной модели ITU МСЭ-R P. 533–13 и результаты его применения для расчёта радиолиний сети КВ-диапазона. Целью данной работы является постановка задачи имитационного моделирования КВ-радиосетей при изменяющихся условиях связи.

Модель прогнозирования условий связи в режиме «Точка-точка»

Программная модель ITU Прогнозирования рабочих характеристик ВЧ-линий, доработана с учётом требований расчёта характеристик всех радиолиний сети на временном интервале длительностью один год. В новом варианте программный и пользовательский интерфейсы модели реализованы средствами программной среды Matlab Пользовательский интерфейс имеет развитые средства управления режимами моделирования радиосети, и графического представления результатов моделирования. Результаты прогнозирования условий связи для радиолиний сети сохраняются в форме таблиц доступных из программы Excel и используются для взаимодействия с программой моделирования модемных цифровых каналов. Исходными данными программной модели Прогнозирований условий связи являются:

– координаты размещения приёмника и передатчика;
– характеристики приёмной и передающей антенны;
– мощность передатчика;
– время (1–24 час); месяц (1–12); год;
– расчётные частоты (до 10);
– солнечная активность.

Расчёт прогнозируемых характеристик радиолиний выполняется по всем заданным частотам, месяцам года и для каждого часа суток. Объем расчётов можно ограничить, конкретно указав желаемые частоты, часы и месяцы. Солнечная активность определяется числом солнечных пятен и устанавливается по номеру года из хранимого файла данных. Программа имеет возможность обновить файл данных солнечной активности через сеть Интернет.

Радиоволны в КВ-диапазоне распространяются за счёт отражения от ионизированных слоёв ионосферы. Закон секанса устанавливает связь между частотами радиоволн, отражающихся от ионосферы при вертикально направленном излучении $f_в$, и частотами радиоволн, отражающихся от той же области ионизации в случае наклонного излучения. Закон описывается выражением:

$$f_{накл} = f_в \sec \varphi_0,$$

где φ_0 — это угол между нормалью к ионосферному слою и направлением падающего на него луча.

Отражающими слоями ионосферы могут быть F1, F2 и E. Слои находятся на разной высоте, наличие слоёв в ионосфере зависит от времени суток и солнечной активности. Отражение возможно от всех слоёв, слой, который обеспечивает максимальный сигнал в точке приёма, называется модой. На рис. 1 показана схема односкачковой

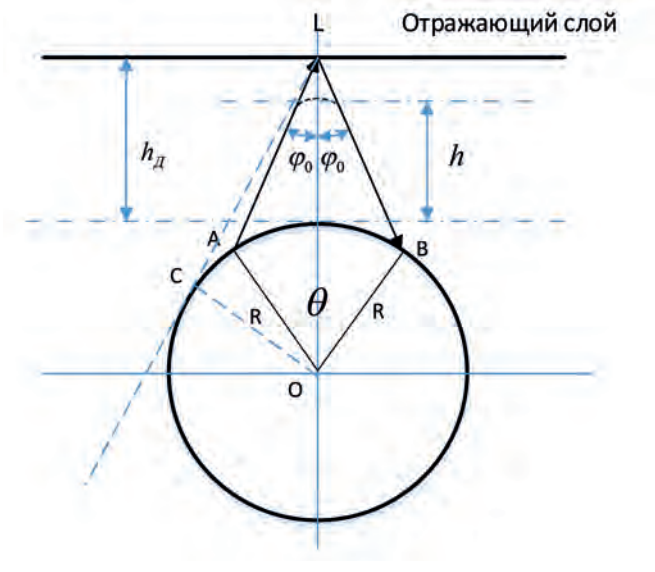

Рис. 1. Схема отражения радиоволны от ионизированного слоя

трассы распространения, дальность односкачковой связи ограничена геометрией Земли (точка С — на рисунке). Предельное значение угла отражения определяется выражением:

$$\sin\varphi_0 = \frac{R}{R + h_D},$$

где R = средний радиус Земли (R = 6371,0 км), h_D — действующая высота отражающего слоя, h — фактическая высота слоя, Ограничение угла φ_0 ведёт к ограничению возможного расстояния односкачковых трасс (2000÷4000 км). На рис. 2 показаны ожидаемые моды распространения по расчётным частотам на июнь 2018 г. для трассы Улан-Уде — Екатеринбург (расстояние 3036 км).

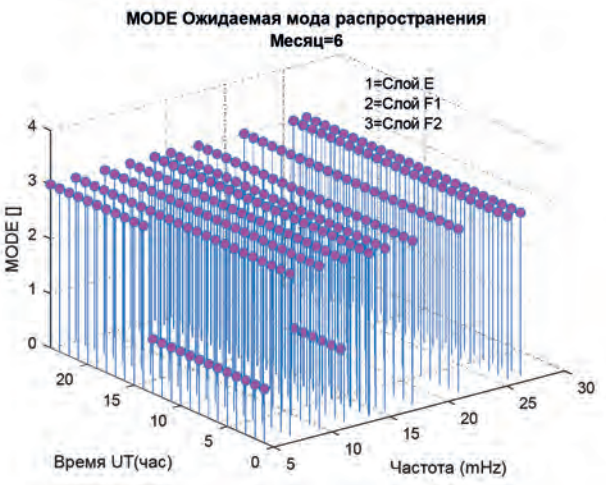

Рис. 2. Ожидаемые моды распространения по расчетным частотам

Возможны также много скачковые трассы, позволяющие радиоволне обогнуть земной шар. В программе моделирования есть возможность выбора расчёта для «короткого» или «длинного» пути. На рис. 3 для этой же трассы показаны количество скачков для расчётных мод «короткого» пути.

1.1. Расчётные характеристики радиолиний

Программная модель Прогнозирования условий связи позволяет получить расчётные значения по следующим характеристикам радиолиний распространения радиоволны:

'MODE' — (Most Reliable Mode propagation mode) ожидаемая мода 'MODEh' — (Number of hops) количество скачков при распространении радиоволны.

'ANGL' — (Elevation angle (deg)) — угол места для наиболее приемлемой моды на данной частоте (в градусах).

'DBU' — (Field strength — dB(1uV/m)) — медиана напряжённости поля, ожидаемая в месте приема взятая по выборке для всех дней месяца. dBu — децибелы относительно микровольта на метр.

'dBpW' — (Median available signal power at receive location (dBpW)). Медиана мощности сигнала, взятая по выборке для всех дней месяца ожидаемая в месте приёма в децибелах относительно пиковатт (picowatt).

'S/N' — (Monthly median signal-to-noise ratio (dB)) — месячная медиана отношения сигнал/шум (S/N) для ожидаемой моды в полосе частот BandWidth (см. rec533–13 п. 7).

'FS/N' — (Calculated reliability) — расчетная надежность. Диапазон [0–0.99].

'SNxx' — (Signal to noise ratio (dB)) — отношение сигнал/шум для требуемой надёжности.

'freq' — (Calculated frequencies (mHz)) — рабочие частоты, используемые при вычислениях.

'LUF' — (Lowest usable high frequency (mHz)) — наименьшая применимая частота рабочей полосы, на которой отношение сигнал/шум достигает значения месячной медианы отношения сигнал/шум (S/N).

'MUFDAY' — оценка надёжности — доля дней в месяце, когда можно ожидать нормальное ионосферное распространение радиоволн для наиболее приемлемой моды обычного луча на данной частоте. Надёжность описывается как вероятность того, что соблюдены указанные критерии рабочих характеристик (т.е. указанное отношение сигнал/шум достигает значения месячной медианы отношения сигнал/шум (S/N)).

'FOT' — (Optimum traffic frequency (mHz)) — оптимальная применимая частота (ОПЧ), наивысшая частота рабочей полосы на которой обеспечивается надёжность радиолинии на уровне 0.90. (MUFDAY = 0.90).

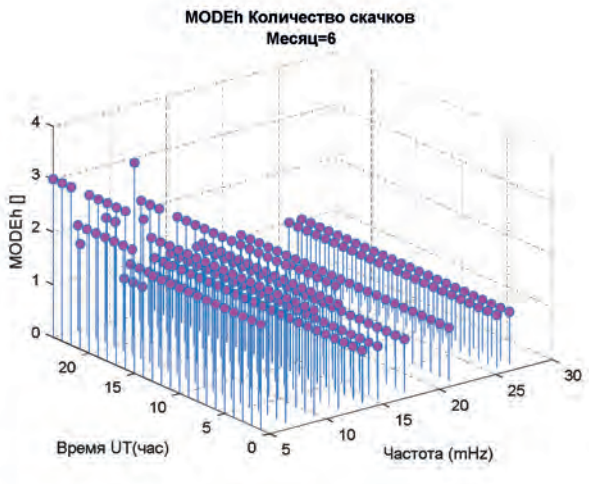

Рис. 3. Количество скачков для расчётных мод

'MUF' — (Maximum usable frequency (mHz)) — максимальная применимая частота (МПЧ) — определяется как частота имеющая значение MUFDAY = 0.50.

'OPMUF' — (Operational MUF (mHz)) — рабочая МПЧ для радиолинии, является наибольшей из рабочих МПЧ для F2-мод и рабочих МПЧ для E мод (см. rec533–13 п. 3.7). Оценка рабочей МПЧ — наивысшей частоты, на которой возможна приемлемая работа радиослужбы, проводится в два этапа: первый состоит в оценке основной МПЧ исходя из рассмотрения параметров ионосферы, а второй — в определении поправочного коэффициента для учёта механизмов распространения на частотах выше основной МПЧ. OPMUF' определяется как частота имеющая значение MUFDAY = 0.10.

Основные МПЧ различных мод распространения оцениваются через соответствующие критические частоты ионосферного слоя и с помощью коэффициента, характеризующего длину скачка.

'MIR' — (Multimode Interference factor (%)) — коэффициент межмодовой интерференции.

'OACR' — (Overall Circuit Reliability (%)) — полная надёжность радиолинии.

'SACR' — (Equatorial Scattering Overall Circuit Reliability (%)) — полная надёжность радиолинии при экваториальном тропосферном рассеивании (см. rec533 п. 10.3).

Результаты расчётов могут быть представлены в шкале локального времени или универсального времени (UT) отсчитываемого на долготе Гринвичского меридиана. На рис. 4 показана медиана мощности сигнала в точке приёма трассы Улан-Уде — Екатеринбург.

На рис. 5 показано отношение сигнал/шум для этой же радиолинии. По завершении расчётов 2D и 3D-графики характеристик можно отобразить в дополнительных ок-

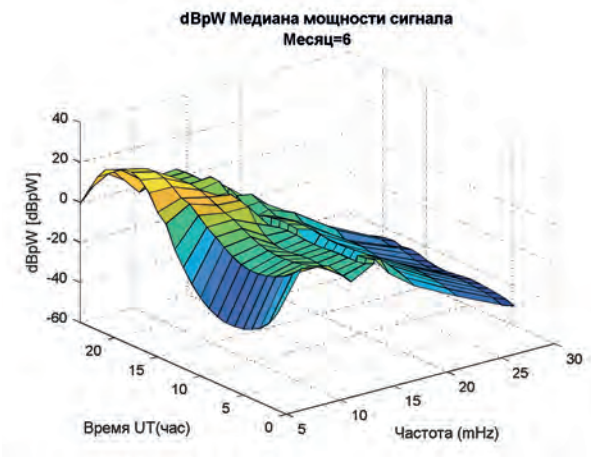

Рис. 4. Мощность сигнала в точке приёма по расчётным частотам

нах. Результаты расчётов могут быть сохранены в виде таблиц в текстовом формате csv.

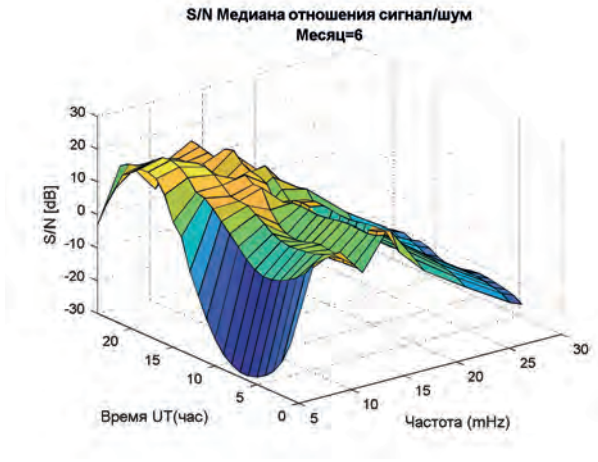

Рис. 5. Отношение сигнал/шум

1.2. Системные параметры радиолинии

Системные параметры распространяются на все радиолинии сети и задаются как исходные данные. В состав системных параметров включаются:

Req. Rel.— (Requires Circuit Reliability (%)) — требуемая надёжность радиолинии, оценивается процентом дней в течение месяца, когда сигнал имеет допустимое качество. Диапазон значений [1–99]%, по умолчанию 90%.

Req. SNR — (Required Signal-to-Noise Ratio (dB)) — требуемое отношение медианы почасовой выборки сигнальной мощности к медиане почасовой выборки шума в полосе 1 Hertz, которую необходимо обеспечить для требуемого типа и качества обслуживания. Диапазон значений [–30–99 dB], по умолчанию 73 dB.

Noise — (Manmade Noise (dBW)) — определяет уровень техногенного шума в приёмнике в dBW (децибел на Ватт) в полосе 1 Hertz на частоте 3 MHz, значение по умолчанию — 145 dBW.

Диапазоны по CCIR Report 258 [1,2,3,4,100–200], где:

1 = –140.4 — промышленный шум;

2 = –144.7 — городской шум;

3 = –150.0 — шум в сельской местности;

4 = –163.6 — шум в местности удалённой от населённых и промышленных зон. В этом диапазоне доминирующим является космический шум.

BandWidth — (Reciver bandwidth (Hz)) — расчётная ширина полосы шума на приёмнике.

Min Angle — (Minimum takeoff angle (deg)) — минимальный угол наклона главного лепестка предающей антенны над горизонтом в градусах. Типичное значение по

умолчанию 0.1 град. Диапазон значений [0–40 deg], при значении 0 устанавливается Angle=3 deg.

Дистанция — путь распространения радиоволны, возможные варианты:

- shot — по кратчайшей дуге;
- long — по максимальной дуге вокруг Земного шара.

Параметры цифровой модуляции (см. rec533–13 п. 10.2.1). Задают характеристики, связанные с многолучевым рассеиванием принимаемого сигнала, к ним относятся:

Ампл. отн.— (Amplitude Ratio (dB)) — амплитудный коэффициенте представляет собой отношение почасовых медиан напряжённости доминантной моды к субдоминантной моде, которое затронет рабочие характеристики системы только в том случае, если будет сопровождаться временной задержкой, выходящей за пределы значения Tw либо частотным рассеянием выше значения Fw.

Частотное окно — (Frequency Window (Hertz)) — Fw: Частотный интервал рассеивания принимаемого сигнала, в рамках которого моды сигнала будут способствовать улучшению рабочих характеристик системы, и за пределами которого рабочие характеристики будут ухудшаться.

Врем. окно — (Time Window)(uSec) — Tw: Временной интервал (в микросекундах) рассеивания принимаемого сигнала, в рамках которого моды сигнала будут способствовать улучшению рабочих характеристик системы, и за пределами которого рабочие характеристики будут ухудшаться.

Модель прогнозирования условий связи в режиме «Зона»

Программная модель предназначена для прогнозирования распространения сигнала в радиозоне. Зона задаётся относительно выбранного центра зоны в градусах или в километрах по направлениям «на Восток», «на Запад», «на Север», «на Юг». Отдельно указывает место размещения передатчика, мощность передатчика и характеристики передающей антенны. Зона покрывается равномерной сеткой, в узлах которой находятся приёмники. Минимальный размер сетки 5×5, максимальный 999×999. Все приёмники имеют совпадающие характеристики антенн. Расчёт производится для 1÷9 возможных вариантов. Варианты отличаются по частоте, номеру месяца, часу суток и солнечной активности. Солнечная активность определяется числом солнечных пятен и устанавливается по номеру года. На рис. 6 показан 3D-график изменения отношения сигнал/шум в зоне размером 1000×1000 км., центром которой является г. Москва.

Передатчик размещён в центре зоны. Зона покрыта сеткой размером 71×71. При отображении характеристик зоны в режиме 2D используется цветовая палитра (рис. 7). В плоскости графика можно интерактивно выбрать точку с желаемой интенсивностью, которая отображается маркером. Координаты выбранной точки и значение характеристики сохраняются в таблице маркеров.

Программа позволяет вычислить в выбранной зоне медианные оценки следующих характеристик:

Ожидаемая мода распространения для каждого узла сетки зоны;

Угол возвышения приёмной антенны в узлах зоны;

'DBU' dB(1uV/m)) — медиана напряжённости поля, ожидаемая в узлах приёма для всех вариантов (в децибелах относительно микровольта на метр);

'S/N' (dB) — месячная медиана отношения сигнал/шум (S/N) в узлах сетки для ожидаемой моды в полосе частот BandWidth для всех расчётных вариантов;

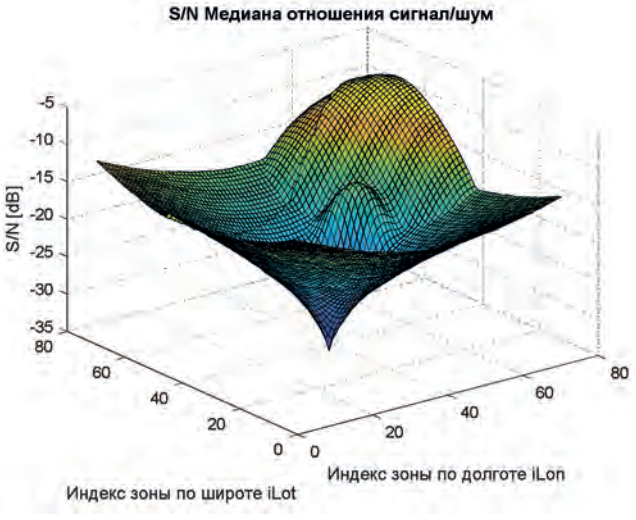

Рис. 6. Функция изменения сигнал/шум в радиозоны 3D представлении

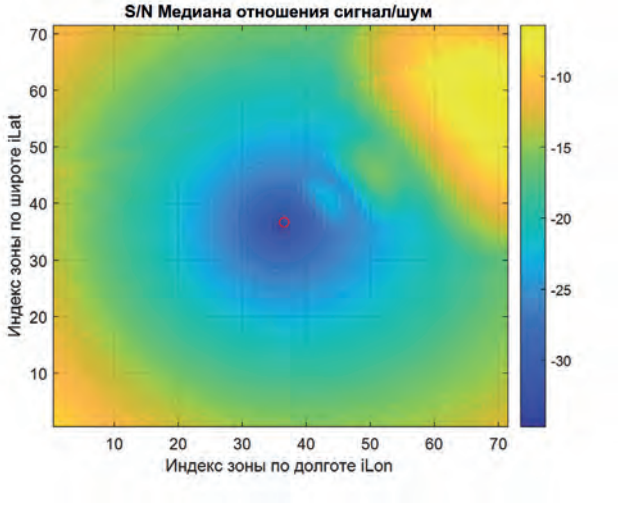

Рис. 7. Функция изменения сигнал/шум в 2D-представлении

'FS/N' — расчётная надёжность радиолиний в узлах сетки. Диапазон [0 ÷ 0.99]. Вероятность того, что отношение сигнал/шум (SNR) превысит требуемое значение (Req. SNR) для всех расчётных вариантов;

'SNxx' (dB) — отношение сигнал/шум в узлах сетки для требуемой надёжности для всех расчётных вариантов.

Радиозона может быть отображена на географической карте в цветовой палитре по значениям характеристики. Интерактивный маркер позволяет определить координаты желаемой точки на карте (рис. 8).

При расчёте радиозоны используются системные параметры, которые задаются также как для программной модели «Точка-точка».

Моделирование радиоканалов

Программная модель радиоканала предназначена для расчёта битовых ошибок и ошибок передачи пакетов по радиолиниям сети при заданных условиях связи. Программа использует модели модемов из МАТЛАБ пакета Communications System Toolbox. Модемы различаются по типам модуляции, размеру алфавита и типам канала. Возможно также подключение моделей модемов, разработанных пользователем. Поддерживаются два типа каналов: AWGN — канал с Гауссовским белым шумом; и Rayleigh and Rician fading — канал с замираниями. По типам используемой модуляции возможны следующие варианты:

- 'psk' — (phase shift keying) фазовая манипуляция;
- 'oqpsk' — (offset quaternary phase shift keying) квадратурная фазовая манипуляция со сдвигом (частоты);
- 'dpsk' — (differential phase shift keying) дифференциальная фазовая манипуляция;
- 'pam' — (pulse amplitude modulation) импульсная амплитудная модуляция;.
- 'qam' — (Quadrature amplitude modulation) квадратурная амплитудная модуляция;.
- 'fsk' — (frequency shift keying) частотная манипуляция;.
- 'msk' — (minimum shift keying) фазо-частотная манипуляция со сдвигом;.
- 'cpfsk' — (continuous phase frequency shift keying) непрерывная фазочастотная манипуляция со сдвигом;.
- 'depsk' — differential Encoded Phase Shift Keying дифференциально-кодированная фазовая манипуляция;

Входными данными программы моделирования являются:

- Таблица отношений сигнал/шум для радиолиний развёрнутая по времени суток и месячным датам;
- Размер алфавита для выбранного типа модуляции;
- Размер пакета, выраженный в битах.

Для каждой радиолинии можно задать свой модем или использовать общий модема для всех радиолиний сети. Выходными данными являются две расчётные таблицы. Формат расчётных таблиц соответствует формату входной таблицы. Первая таблица в столбцах рабочих

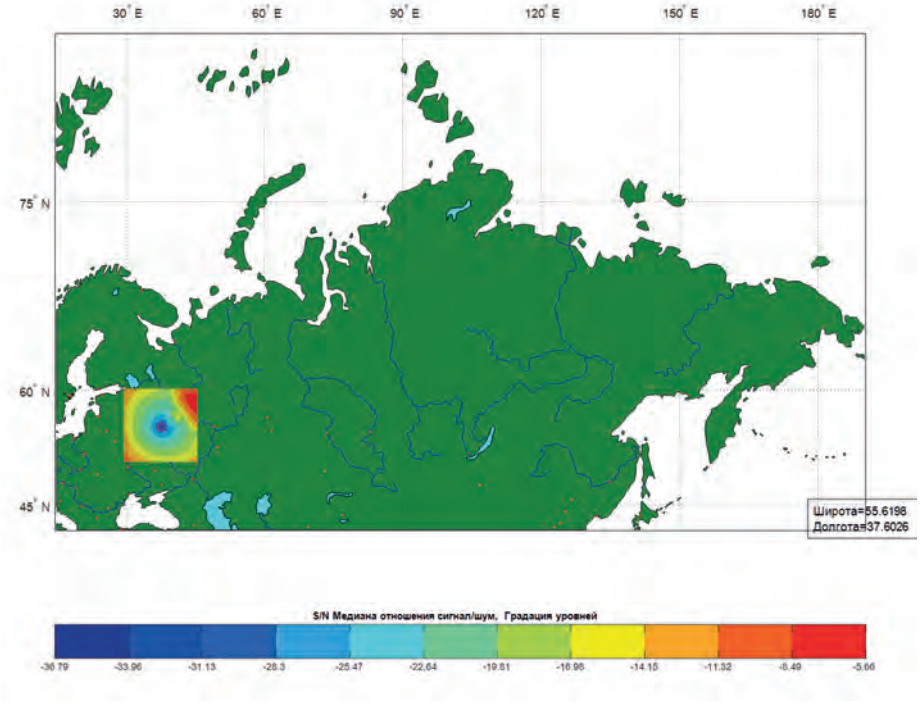

Рис. 8. Отображение радиозоны на географической карте

частот содержит вероятности битовых ошибок, вторая таблица в столбцах рабочих частот содержит вероятности ошибок при передаче пакета. Размер пакета задаётся в пользовательском интерфейсе.

В цифровых системах передачи, особенно при сравнении различных методов исправления ошибок, принято использовать нормированное отношение средней энергии на бит информации к спектральной плотности мощности шума E_b/N_0. Это отношение, выраженное в децибелах, используется в функциях пакета Communications System Toolbox при расчете битовых ошибок. Отношение удобно тем, что в нем не фигурируют абсолютные значения полосы частот и длительности тактового интервала.

Обозначим через S — среднею мощность сигнала. Мощность шума при передаче сигнала в полое B_s равна $N = N_0 B_s$. Спектральная плотность мощности шума N_0 имеет размерность энергии. Соответствие между E_b/N_0 и S/N выраженное в децибелах имеет вид:

$$\left(E_b/N_0\right)_{DB} = \left(S/N\right)_{DB} - 10\log_{10}\left(Log_2 L\right),$$

где L — размер алфавита (позиционность модуляции). График зависимости битовой ошибки от значения E_b/N_0 при работе с модуляцией ‘gam’ и алфавитом k=4 в канале AWGN показан на рис. 9. Значения уровня шума S/N для данного модема больше значения E_b/N_0 на величину 3.0103 dB.

На рис. 10 показано значение битовых ошибок в 3D-представлении для модема с модуляцией ‘gam 4’, в канале AWGN на максимально применимой частоте (MUF). Пики графика в координатах месяц-час соответствуют отсутствию прохождения радиосигнала между абонентами радиолинии Хабаровск-Екатеринбург.

Программная модель службы ИВ-ЧДС

При работе в сетевом окружении необходимой составляющей организации системы связи является Ионосферно-Волновая Частотно-Диспетчерская служба (ИВ-ЧДС). Служба предназначена для построения волнового расписания всех радиолиний радиосети КВ-диапазона по данным радиопрогноза условий связи. Программная модель позволяет выполнить построение двух типов волнового расписания: многочастотного и двухчастотного.

Многочастотное расписание — изменение рабочей частоты происходит каждый час. Частота выбирается из списка рабочих частот, передача данных на которых не превышает допустимый уровень ошибки. Выбор осуществляется по минимальному значению ошибки пакета. В случае равенства ошибок выбирается наибольшая частота. Если для всех рабочих частот текущего часа уровень ошибки меньше порогового, то значение частоты принимается равным нулю (это является индикатором нарушения допустимых условий связи), а уровень ошибки устанавливается по минимальному по всем частотам значению ошибки пакета.

Двухчастотное расписание — используются две рабочих частоты: дневная и ночная. Смена частот происходит на границе между днём и ночью. На временных интервалах дня и ночи выбирается частота, на которой уровень ошибки не превышает допустимый. Приоритет имеют частоты с наибольшим числом часов работы при допустимой ошибке. При равенстве приоритетов выбирается частота, имеющая наибольшее значение. Если для выбранной частоты на некотором часовом интервале уровень ошибки превышает допустимый, то для этого интервала значение частоты принимается равным нулю, а уровень ошибки устанавливается по фактическому значению для данного часа.

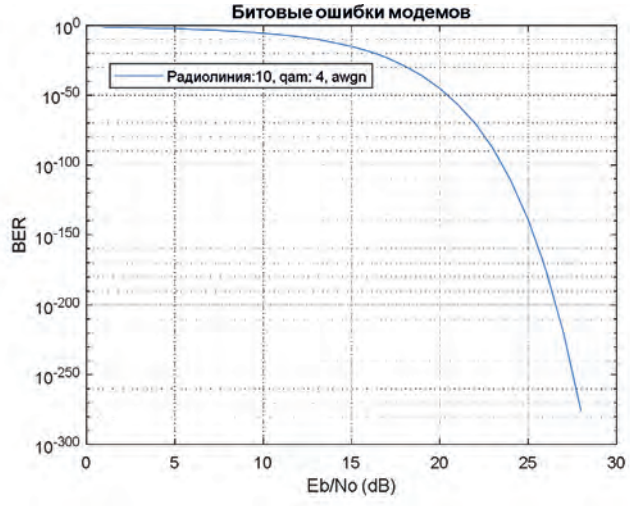

Рис. 9. Битовые ошибки для модема с модуляцией ‘gam’ и алфавитом k=4 в канале AWGN

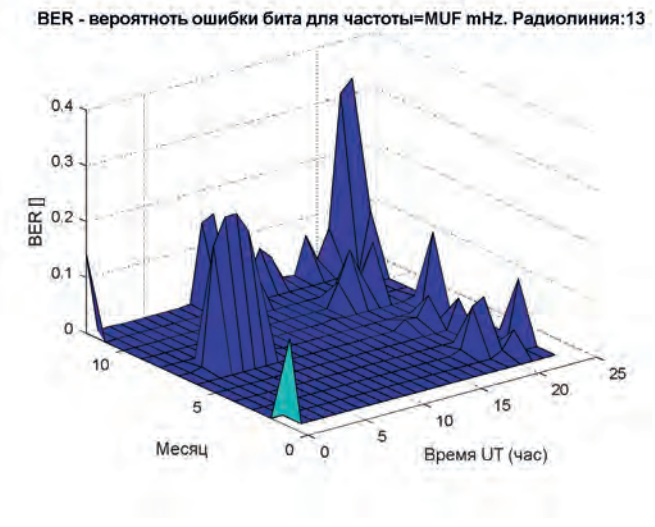

Рис. 10. Ошибки BER для трассы Хабаровск-Екатеринбург

На рис. 11 показано волновое двухчастотное расписание для трассы Хабаровск-Екатеринбург на октябрь 2018 г.

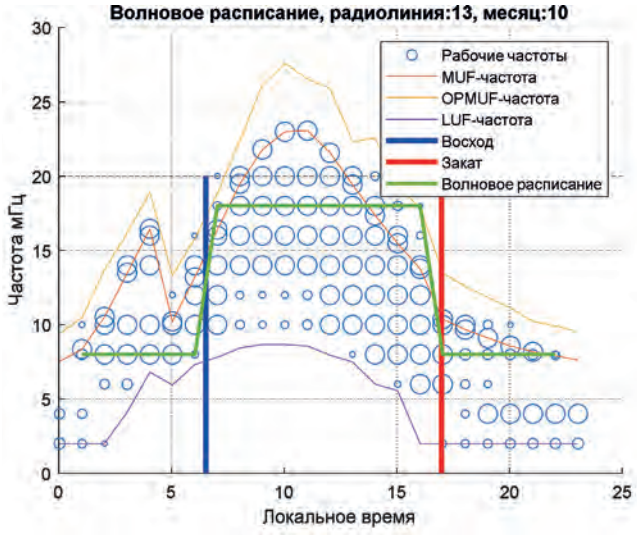

Рис. 11. Двухчастотное волновое расписание для трассы Хабаровск-Екатеринбург

При отображении, размер маркеров на графике указывают допустимые рабочие частоты на приёмной стороне радиолинии. Чем больше размер маркера, тем выше качества канала (тем меньше уровень ошибки пакета). На рис. 12 показано многочастотное волновое расписание для той же трассы.

Модель позволяет также оценить суточную связанность для радиолинии сети по пороговому уровню ошибки на пакет. На рис. 13 показана диаграмма суточной связанности радиолиний для 7 месяца 2018 г. при пороговом уровне вероятности пакетной ошибки 0.001.

По горизонтальной оси отложено универсальное время, отсчитываемое на долготе Гринвичского меридиана. В пустых позициях диаграммы «зонах молчания» уровень пакетных ошибок выше допустимого, что можно считать отсутствием связи требуемого качества. Точки на диаграмме соответствуют достаточному уровню качества на приёмной стороне (Екатеринбурге). На рис. 14 показано многочастотное волновое расписание для линии Хабаровск-Екатеринбург (13 радиолиния) на 7 месяц 2018 г.

Сдвиг «зоны молчания» на последнем рисунке по отношению к «зоне молчания» 13 радиолинии на рис. 13

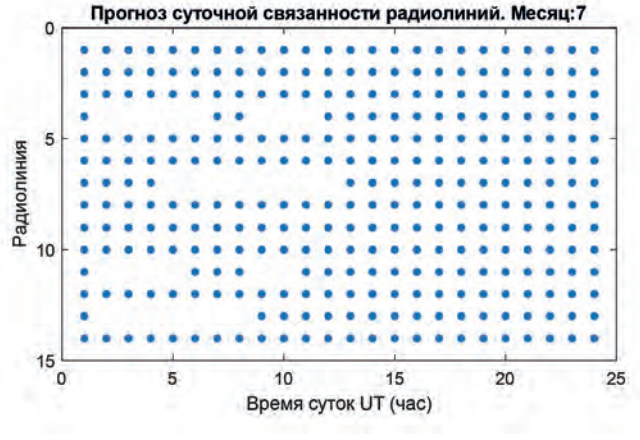

Рис. 13. Диаграмма суточной связанности радиолиний сет

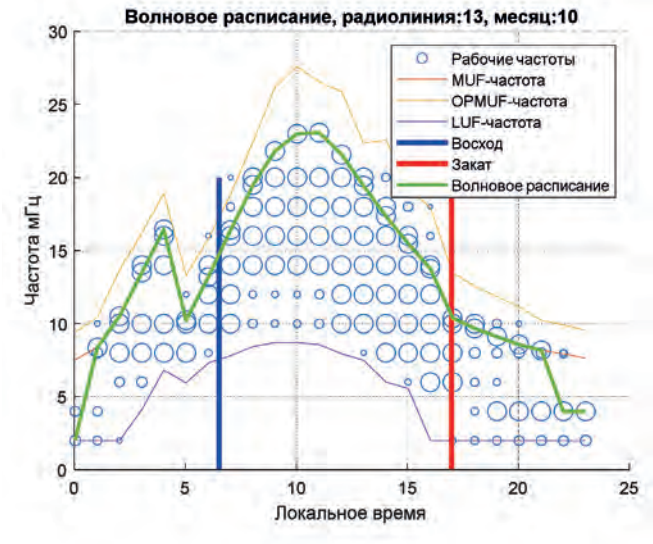

Рис. 12. Многочастотное волновое расписание для трассы Хабаровск-Екатеринбург

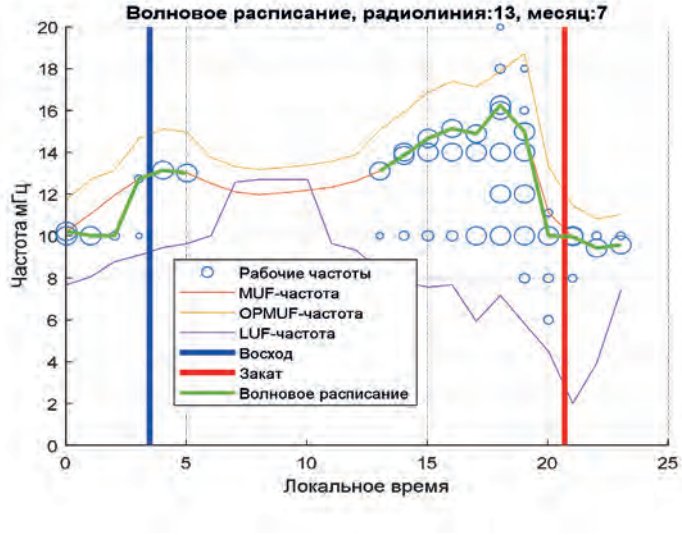

Рис. 14. Многочастотное волновое расписание Хабаровск-Екатеринбург на 7 месяц 2018 г.

обусловлен сдвигом на 4.2 часа локального времени места размещения приёмника по отношению к универсальному времени. Интерфейс модели позволяет установить календарную дату, выбрать границу сумерек, установить размер пакета, установить пороговое значение ошибки на пакет, показать географические координаты преемника и передатчика, время восхода, заката и часовой пояс, загрузить таблицу радиолиний сети и таблицу битовых ошибок. Построенное волновое расписание можно сохранить в текстовом файле в виде таблицы.

Схема моделирования процесса работы пакетной радиосети

Схема моделирования процесса работы пакетной сети показана на рис. 15. Цель моделирования заключается в оценке основных вероятностно-временных характеристик КВ-радиосети по передаче сообщений и эффективности выбранных протоколов взаимодействия при работе радиолиний в пакетном режиме в условиях изменяющихся условий связи. Взаимодействие моделей осуществляется через общую память или файловую систему.

Рис. 15. Схема моделирования процесса работы радиосети

Исходные данные по району размещения сети представлены в геомодели местности. На геомодель наложена топологическая модель радиосети, определяющая связи между сетевыми узлами. Модель Прогнозирования условий связи производит почасовой расчёт прогноза отношения сигнал/шум по рабочим частотам (а также максимально-применимой частоте MUF) для всех радиолиний сети на период от 1 до 12 месяцев года. Модель радиоканала использует эти данные для расчёта битовых ошибок и ошибок на пакет по радиолиниям сети во временном пространстве час-месяц. Программная модель ИВ-ЧДС использует таблицу битовых ошибок для расчёта волнового расписания по радиолиниям. Волновое расписание работы радиолиний, топология сети и гео-данные района размещения сети загружаются в имитационную модель пакетной радиосети. Эта модель выполняет имитационное моделирование пакетной сети радиосвязи в расчётном временном интервале с модельной длительностью до одного года. По выбранной нагрузке на сеть устанавливаются интенсивность генерации пакетов данных на узлах сети. Результатом моделирования являются вероятностно-временные характеристики (ВВХ) работы сети на расчётном временном интервале. В состав ВВХ включаются характеристики надёжности, достоверности и своевременности доставки пакетов и сообщений через сеть.

Заключение

Имитационное моделирование является базовым средством разработки телекоммуникационных сетей, позволяющим оценить характеристики и выбрать настроечные параметры протоколов передачи данных для беспроводных мобильных сетей. Для задач проектирования радиосети необходимо иметь оценки ВВХ при изменяющихся условиях связи за достаточно длительный временной интервал. Для КВ-диапазона это особенно актуально, поскольку период стационарности ионосферы редко превышает 20 мин. Рассмотренный моделирующий комплекс включает модели всех базовых составляющих КВ-радиосети передачи данных, что позволяет получить статистические характеристики сети близкие к реальным.

Результаты моделирования дают возможность рациональным образом выбрать параметрическую область решений, удовлетворяющую нормативным требованиям.

Литература

1. *Крашенинников И.В., Павлова Н.М., Ситнов Ю.С.* Модель IRI: Анализ среднемесячных параметров в задаче прогнозирования ионосферного прохождения радиоволн в условиях высокой солнечной активности // Гелиогеофизические исследования: Специальный выпуск. 2016. No. 14. С. 82–91.

2. *Гуляева Т.Л.* Модификация индексов солнечной активности в международных справочных моделях ионосферы IRI и IRI-Plus в связи с пересмотром ряда солнечных пятен // Солнечно-земная физика. 2016. Т. 2. № 3. С. 59–68.

3. *Анишин М.М., Радио Л.П.* Опыт применения ионосферной модели IRI-2012 для прогнозирования МПЧ на ВЧ-трассах // Гелиогеофизические исследования. 2015. No. 11 С. 13–18.

4. *Дорогов А.Ю.* МАТЛАБ интерфейс к программной модели ионосферы IRI-2016 // Материалы V межрегиональной научно-практической конф. «Перспективные направления развития отечественных информационных технологий» (Севастополь, 24–28 сентября 2019 г.). Севастополь: СевГУ, 2019. С. 238–240.

5. *Кизима С.В., Ладанов М.В.* Ионосферное обеспечение радиосвязи и радиомониторинга в декаметровом диапазоне частот (1.5 1,5–30 мГц) // Электросвязь. 2013. № 7. С. 1–4.

6. *Завадский С.В., Путилин А.Н., Сиротинин И.В.* Многочастотный имитатор КВ канала для адаптивной системы КВ радиосвязи с псевдослучайной перестройкой рабочей часто-

ты // Сборник XX Международной научно-технической конференции «Радиолокация, навигация и связь». 2014. С. 937–942.

7. *Ладанов М.В., Ведищев А.М., Кизима С.В., Лавров Г.В.* Планирование радиосвязи на коротких волнах для магистральных радиотрасс // Электросвязь. 2012. № 9. С. 3–8.

8. *Стругов Ю.Ф., Семенов А.М., Добровольский С.М., Батырев И.А.* Стохастическое моделирование каналов с аддитивными и мультипликативными помехами. Схема реализации // Математические структуры и моделирование 2015. № 2(34). С. 48–63.

9. *Анишин М. М., Радио Л.П.* Программный комплекс для прогнозирования характеристик КВ-радиолиний «Трасса-2019» (часть 1) // Техника радиосвязи. 2019. Вып. 4 (43). С. 14–26. 10. *Дорогов А.Ю., Потапов И.А., Тутене А.С.* Модели-рование протоколов беспроводных сетей в среде Матлаб // Наукоемкие технологии в космических исследованиях Земли. 2019. № 3. С. 32–45.

SOFTWARE PACKAGE FOR MODELING HF-BAND PACKET RADIO NETWORKS

ALEKSANDER YU. DOROGOV

Saint Petersburg, Russia, vaksa2006@yandex.ru

ALEKSANDR I. YASHIN

Saint Petersburg, Russia, vaksa2006@yandex.ru

KEYWORDS: ionosphere; radio line; digital modem; radio zone; radio network; applicable frequencies; signal-to-noise ratio; wave schedule.

ABSTRACT

It is noted that the complexity and constant variability of the ionosphere structure, the presence of many factors affecting the propagation of radio waves in such an environment, as well as the complex topology of communication networks lead to the need the computer modeling of data transmission in HF-band networks. The existing models of representation of ionospheric processes and digital radio channels are described. It is shown that to solve the problems of designing a radio data transmission network, complex modeling is necessary, taking into account the network topology, signal propagation losses in the radio channel, noise level, type of digital modulation, and radio forecast of communication conditions. In this paper, we consider a modeling complex for packet radio networks of HF-band data transmission with changing communication conditions. The complex consists of a set of interacting models implemented in the Matlab software environment. The software model for predicting communication conditions complies with ITU-R recommendation P. 533-13 of the International Telecommunication Union (ITU). The description of the model for the "Point-to-point" and "Area" modes is given and the results of its application for calculating extended radio lines are shown. The initial data and system parameters of the model are described. A model of the HF-band digital radio channel is presented. The communications System Toolbox package, which is part of the Matlab software environment, is used for this modeling. The model's input and output data are described. A model of Ionospheric Wave Frequency Dispatcher service of the radio network has been developed. This model is intended for building a wave schedule for stable operation of HF radio lines in the network. The rules for building a two-frequency and multi-frequency wave schedule are described. A scheme for modeling the operation of a packet radio network under changing communication conditions is proposed. The complex allows you to evaluate the probabilistic and temporal characteristics of radio lines and zonal radio coverage depending on geographical coordinates, time, month, solar activity and selected system parameters for a period of up to one year. Examples of using the modeling complex are given. The purpose of this work is to formulate the problem of simulation of HF radio networks under changing communication conditions.

REFERENCES

1. Krasheninnikov I.V., Pavlova N.M., Sitnov Yu.S. Model IRI: analysis of month mean parameters in the problem of point-to-point ionospheric radio waves propapagation in the high solar activity conditions. *Heliogeophysical research*. 2016. No. 14. Pp. 82–91. (In Rus)

2. Gulyaeva T.L. Modification of the solar activity indices in the international reference ionosphere iri and iri-plas models due to recent revision of sunspot number time series. *Solnechno-zemnaya fizika*. 2016. Vol. 2. No. 3. Pp. 59–68. (In Rus)

3. Anishin M.M., Radio L.P. The international reference ionosphere IRI-2012 using experience for MUF prediction on HF communication channel. *Heliogeophysical research*. 2015. No. 11. Pp. 13–18. (In Rus)

4. Dorogov A. Yu. MATLAB interface to software model of the ionosphere IRI-2016. *Advanced national information systems and technologies Materials of V interregional scientific-practical conference* (Sevastopol, September 24-Kizima S.V., Ladanov M.V. Ionospheric provision of radio communications and radio monitoring in the de-

cameter frequency range (1.5 1,5–30 mGc). *Elektrosvyaz'* [Telecommunication]. 2013. No. 7. Pp. 1–4. (In Rus)
5. Zavadskiy S.V., Putilin A.N., Sirotinin I.V Multifrequency HF channel simulator for adaptive HF radio with a pseudorandom restructuring operating frequency. *Sbornik trudov Radiolokacija, navigacija i svjaz' XX Mezhdunarodnaja nauchno-tehnicheskaja konferencija* [Proc. of the Radar, navigation and communication XX international scientific and technical conference]. 2014. Pp. 937–942. (In Rus)
6. Ladanov M.V., Vedishhev A.M., Kizima S.V., Lavrov G.V. Planning of short-wave radio communications for trunk radio routes. *Elektrosvyaz'* [Telecommunication]. 2012. No. 9. Pp. 3–8. (In Rus)
7. Strugov Ju.F., Semenov A.M., Dobrovol'skij S.M., Batyrev I.A. Stochastic simulation of the radio channel with additive and multiplicative line noises. implementation scheme. *Matematicheskie struktury i modelirovanie* [Mathematical structures and modeling]. 2015. No. 2(34). Pp. 48–63. (In Rus)
8. Anishin M.M., Radio L.P. Software package for forecast characteristics hf radio link "TRASSA-2019". *Tehnika radiosvjazi* [Radio communication technology]. 2019. No. 4 (43). Pp. 14–26. DOI 10.33286/2075–8693–2019–43–14–26. (In Rus)
9. Dorogov A. Yu., Potapov I.A., Tutene A.S. Modeling of wireless network protocols in the environment of MATLAB. *H&ES Research*. 2019. No. 3. Pp. 32–45. DOI: 10.24411/2409–5419–2018–10267 (In Rus)

INFORMATION ABOUT AUTHORS:
Dorogov A.Yu, PhD, Docent, Chief researcher of JSC "Information and telecommunication technologies ("Inteltech")" ;
Yashin A.I., PhD, Full Professor, Associate Director of JSC "Information and telecommunication technologies ("Inteltech")"

For citation: Dorogov A.Yu, Yashin A.I. Software package for modeling HF-band packet radio networks. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 26–37. doi: 10.36724/2409-5419-2020-12-6-26-37 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-38-47

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТЕГОСИСТЕМ С ВЛОЖЕНИЕМ В НАИМЕНЬШИЕ ЗНАЧАЩИЕ БИТЫ С СОГЛАСОВАНИЕМ И С ЗАМЕЩЕНИЕМ

АХРАМЕЕВА
Ксения Андреевна[1]

ГЕРЛИНГ
Екатерина Юрьевна[2]

АННОТАЦИЯ

В работе представлены результаты сравнительного анализа стегосистем с алгоритмами вложения в наименьший значащий бит с согласованием и с замещением на предмет различия процедуры вложения дополнительной информации в покрывающий объект и стойкости полученных стеганограмм к различным методам стегоанализа. При использовании стегосистем с алгоритмами вложения в наименьший значащий бит с согласованием и с замещением получены выборки стеганограмм с различными долями вложения по взятой выборке из 200 покрывающих объектов. Проанализированы результаты стегоанализа на данные стеганограммы, произведено сравнение полученных выборок стеганограмм к обнаружению наличия вложения дополнительной информации, при помощи трех методов стегоанализа: визуальной атаки, статистической атаки первого порядка (атака хи-квадрат) и статистической атаки второго порядка (атака парно-выборочного анализа). Представленный пример изображений до и после визуальной атаки, для выборок стеганограм с вложениями в наименьший значащий бит с замещением и с согласованием, при долях вложения в 10%, 50% и 100%, позволяет наглядно продемонстрировать результативность визуального метода стегаонализа. Графическая форма представления результатов по атакам первого и второго порядков позволяет оценить эффективность исследуемых методов стегоанализа для стегосистем с алгоритмами вложения в наименьший значащий бит с согласованием и с замещением. Показано, что стегосистема с алгоритмом вложения в наименее значащие биты с согласованием является более устойчивой к атакам обнаружения, использующим современные методы стегоанализа. Сделаны выводы о возможности применения рассмотренных методов стегоанализа к представленным методам стегосистем.

Сведения об авторах:

[1]к.т.н., доцент Санкт-Петербургского государственного университета телекоммуникации им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, oklaba@mail.ru

[2]к.т.н., доцент Санкт-Петербургско гогосударственного университета телекоммуникации им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, gerlingeu@gmail.com

КЛЮЧЕВЫЕ СЛОВА: стеганография; вложение в наименьшие значащие биты; стегоанализ; покрывающий объект; стеганограмма.

Для цитирования: *Ахрамеева К.А., Герлинг Е.Ю.* Сравнительный анализ стегосистем с вложением в наименьшие значащие биты с согласованием и с замещением // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 38–47. doi: 10.36724/2409-5419-2020-12-6-38-47

Введение

Защита частной информации является основной задачей стеганографии. Это один из наиболее древних и распространённых методов сокрытия информации, суть которого заключается в маскировке защищаемой информации внутри других, безобидных невинных данных (покрывающий объект) [1]. После вложения скрываемой информации в покрывающий объект получается стеганограмма (либо стегообъект). Стеганография определяется как наука сокрытия информации таким образом, чтобы существование вложенной информации не обнаруживалось посторонним наблюдателем или программным обеспечением[1].

В современном мире активно развивается цифровая стеганография, позволяющая скрывать информацию в покрывающих объектах, которые представляют собой оцифрованную информацию, например, в компьютерных файлах различных форматов, в заголовках пакетов различных протоколов и т.д. [2] Компьютеры и компьютерные сети передачи данных прочно вошли в нашу жизнь. Объемы информации в цифровом виде, в том числе конфиденциальной, личного характера, представляющей коммерческую тайну и т.д., хранящейся и передающейся по современным сетям, растут каждый день. Защита этих данных от несанкционированного прочтения, удаления или использования сегодня является актуальной и остро стоящей задачей. Для построения надежной и безопасной информационной системы с хранением и передачей информации необходимо неуклонно соблюдать три принципа — конфиденциальность, целостность и доступность[2]. Для обеспечения конфиденциальности, т.е. для защиты личных данных, коммерческой тайны и т.д. все чаще применяются методы цифровой стеганографии. Поэтому на сегодняшний день развитие, исследование, сравнения и разработка новых методов стеганографии также является актуальной задачей. Но при этом методы стеганографии могут быть использованы и для незаконного обмена информацией, например, для распространения нелегального контента, для общения террористическими группировками и т.д. Поэтому остро также стоит и вопрос выявления скрытой информации в невинных объектах. Для выявления скрытой информации активно разрабатываются методы стегоанализа.

В данной работе далее речь пойдет именно о цифровой стеганографии, для краткости будем называть ее просто «стеганография».

Наиболее распространенным и одним из самых простых методов построения стегосистем является метод вложения в наименьшие значащие биты отсчетов покрывающего объекта. На сегодняшний момент наиболее распространенными являются два метода стегосистем с вложением в наименьшие значащие биты: стегосистемы с вложением в наименьшие значащие биты с замещением (СГ-НЗБ) и стегосистемы с вложением в наименьшие значащие биты с согласованием (СГ-±1-НЗБ). Согласно ранее проведенным исследованиям [3] именно эти два метода чаще всего встречаются в современном программном обеспечении, использующем методы стеганографии.

Также согласно все там же исследованиям в качестве покрывающих объектов, как правило, используются медиафайлы с неподвижными изображениями [4]. Поэтому далее в данной работе в качестве объектов исследования использованы файлы с неподвижными изображениями [5].

Описание стегосистемы с вложением в наименьшие значащие биты с замещением

Рассмотрим метод вложения в наименьшие значащие биты с замещением (СГ-НЗБ) на примере неподвижного растрового изображения[3].

Алгоритм вложения СГ-НЗБ очень прост, если необходимо вложить бит информации, равный 1, то наименее значащий бит пикселя меняется на 1 (вне зависимости от того, какой именно бит там был в покрывающем объекте). Если необходимо вложить бит информации, равный 0, то наименее значащий бит пикселя меняется на 0 [6].

Покрывающий объект можно представить в виде последовательности L-битовых отсчетов

$$C(n) = \sum_{i=0}^{L-1} C_i(n)2^i,$$

где $C(n)$ — это отсчеты покрывающего объекта;

n — количество отсчетов в покрывающем объекте;

$L = 2^t$ — количество уровней;

t — количество биты на пиксель (поскольку в работе рассматривается пример с неподвижным растровым изображением);

$C_i(n) = 0,1$ — двоичные коэффициенты.

После вложения дополнительной информации гистограмма изображения примет вид:

$$C_w(n) = \sum_{i=1}^{L-1} c_i(n) \cdot 2^i + b(n),$$

где $C_w(n)$ — это отсчеты стеганограммы;

$b(n)$ — погружаемый в n-ый отсчет бит информации $b \in (0,1)$.

[1]Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-ПРЕСС, 2016. 262 с.

[2]Рябко В.Я., Фионов А.Н. Основы современной криптографии и стеганографии. М.: Горячая линия, Телеком, 2010. 232 с.

[3]Fridrich J. Steganography in Digital Media Principles, Algorithms, and Applications. Cambridge UnivP, 2010. 462 p.

Пример: Имеется изображение с градациями яркости $L = 256$, $t = 8$ (8 бит на пиксель).

$C(n) = 00101101 = 45$ (пиксель имеет яркость 45).

Если вкладываемый бит $b(n) = 0$, то в стеганограмме получаем уровень яркости $C_w(n) = 00101100 = 44$.

Если вкладываемый бит $b(n) = 1$, то в стеганограмме получаем уровень яркости $C_w(n) = 00101101 = 45$.

Таким образом, последний бит при вложении 1 заменяется на 1, а при вложении 0 — на 0. В примере, в каждый пиксель можно вложить один бит информации.

Процесс извлечения вложенных бит можно представить следующим выражением:

$$\begin{aligned}&\tilde{b}(n) = 0, \text{ если } C_w(n) - \text{четное число, т. е. НЗБ } \left(C_w(n)\right) = 0;\\ &\tilde{b}(n) = 1, \text{ если } C_w(n) - \text{нечетное число, т. е. НЗБ } \left(C_w(n)\right) = 1.\end{aligned} \quad (1)$$

Как следует из формулы (1), если наименьший значащий бит в пикселе стеганограммы равен 1, то извлекается 1, если 0 — то 0.

Описание стегосистемы с вложением в наименьшие значащие биты с согласованием

Процедура вложения для стегосистемы с вложением в наименьшие значащие биты с согласованием (СГ-±1-НЗБ) имеет следующий вид[4]:

$$C_w(n) = \begin{cases} C(n), \text{ если НЗБ } (C(n)) = b(n);\\ \left.\begin{matrix} C(n)+1, \text{ с вероятностью } 1/2\\ C(n)-1, \text{ с вероятностью } 1/2 \end{matrix}\right\}, \text{ если НЗБ } (C(n)) \neq b(n). \end{cases} \quad (2)$$

Из выражения (2) видно, что вложение представляет собой рандомизированный алгоритм.

Пример. Допустим, имеется цифровое изображение, в котором $x_5 = 228$, $x_6 = 202$, $x_7 = 202$. Что в двоичном представлении соответствует $x_5 = 11100100$, $x_6 = 11001010$, $x_7 = 11001010$. Например, необходимо передать сообщение, представленное битами 011. Тогда встраиваемая последовательность бит будет, соответственно, $m_5=0$, $m_6=1$, $m_7=1$. Следовательно, соответствующие яркости пикселов стеганограммы будут: $x_5 = 11100100$ ($x_5 = 228$), $x_6 = 11001001$ ($x_6 = 201$), $x_7 = 11001011$ ($x_7 = 203$).

Таким образом, в СГ-±1-НЗБ в процессе вложения дополнительной информации младший (наименьший значащий) бит, также как и в предыдущем методе, изменяется в зависимости от соответствующего бита встраиваемого сообщения, но при этом происходит «сглаживание» новой, полученной после вложения, гистограммы. «Сглаживание» достигается за счет того факта, что при вложении битов информации со значением 1, яркость будет увеличиваться и уменьшаться с равной вероятностью, и перераспределение значений количества пикселей будет происходить не между двумя соседними отчетами, как в СГ-НЗБ, а между 3 следующими друг за другом отчетами.

Описание методов стегоанализа

В данной работе рассмотрим 3 основных метода стегоанализа на стегосистемы с вложением в наименьшие значащие биты, основанные на статистических свойствах исследуемого объекта [8,9]:

1. визуальная атака;
2. статистическая атака первого порядка;
3. статистическая атака второго порядка

Для проведения сравнительного анализа применим приведенные выше атаки и к СГ-НЗБ и к СГ-±1-НЗБ.

Для проведения визуального стегоанализа необходимо привести исследуемое изображения (цветное или в градациях серого) к черно-белому. Для перевода изображения к черно-белому необходимо воспользоваться следующим алгоритмом:

$$\text{если } C_0(n) = 1, \text{то } \tilde{C}(n) - \text{белое};$$
$$\text{если } C_0(n) = 0, \text{то } \tilde{C}(n) - \text{черное},$$

где $C_0(n)$ — значение наименьшего значащего бита n-го пикселя;

$\tilde{C}(n)$ — значение пикселя в новом черно-белом изображении.

Далее, как правило, необходимо присутствие человека, который визуально рассмотрит полученное черно-белое изображение. Если на полученном черно-белом изображении видны контуры оригинального изображения, то следует сделать вывод, что вложения нет. Если вместо контуров исходного изображения виден шум — делается вывод, что дополнительное вложение есть. Основным недостатком данного метода является сложный механизм автоматизации (пример автоматизации визуального метода рассмотрен, например, в [10]) и, как следствие, необходимость присутствия человека-оператора, для принятия окончательного решения о наличии или отсутствии вложения в исследуемом объекте.

Статистическая атака первого порядка — атака хи-квадрат сводится к расчету параметра χ^2:

$$\chi^2 = \sum_{j=0}^{\left[(L-1)/2\right]} \frac{\left(n_{2j} - n_{2j+1}\right)^2}{2\left(n_{2j} + n_{2j+1}\right)},$$

где n_{2j} — это количество пикселей оттенка $2j$;

n_{2j+1} — это количество пикселей оттенка $2j+1$;

[4]Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография: монография. СПб.: СПбГУТ, 2016. 226 с.

L — это общее количество пикселей в исследуемом изображении.

Критерий обнаружения стегосистем с вложением в наименьшие значащие биты будет иметь следующий вид:

$$H_0 : \chi^2 \geq \chi_0^2;$$
$$H_1 : \chi^2 < \chi_0^2,$$

где H_0 — гипотеза, при которой вложение дополнительной информации отсутствует;

H_1 — гипотеза, при которой вложение дополнительной информации присутствует;

χ_0^2 — это некоторое пороговое значение, которое необходимо выбрать заранее.

Стегоанализ на основе статистики второго порядка был впервые предложен в работе [3]. Данный метод стегоанализа разрабатывался для обнаружения вложений, выполненных методом СГ-НЗБ. Еще одно название данного метода sample pair analysis — парно-выборочный анализ.

Для атаки методом парно-выборочного анализа критерий обнаружения имеет следующий вид:

$$H_0 : \tilde{P} \leq \tilde{P}_0;$$
$$H_1 : \tilde{P} > \tilde{P}_0,$$

где $\tilde{P}_0$ — это пороговое значение, в [12] рекомендуется в качестве порогового значения использовать «0»; а параметр $\tilde{P}$ рассчитывается по следующему правилу:

$$\tilde{P} = \frac{\frac{2D_0 + 2Y_1 - D_2 - 2X_1}{2}}{\frac{2C_0 - C_1}{2}} - \frac{\sqrt{\left(-\frac{2D_0 + 2Y_1 - D_2 - 2X_1}{2}\right)^2 - 4\frac{2C_0 - C_1}{4}(Y_1 - X_1)}}{\frac{2C_0 - C_1}{2}},$$

где C_0 — это количество пар, которые совпадают в первых семи битах;

C_1 — количество пар, которые отличаются на 1 в первых семи битах;

D_0 — это количество пар, которые совпадают во всех битах;

D_2 — это количество пар, которые отличаются на 2;

X — это количество пар вида ($2k$, $2k$-1), где k — целое число;

Y — это количество пар вида ($2k$+1, $2k$), где k — целое число.

Особенность метода парно-выборочного анализа заключается еще и в том, что при малых (менее 10%) долях вложенной информации значение $\tilde{P}$ показывает оценку доли вложенной информации. Данное значения позволяет оценить количество скрываемой информации, которая передается в исследуемой стеганограмме.

Практические результаты

Исследование проводилось на выборке из 200 изображений, которые являются покрывающими объектами. В изображения из выборки было произведено вложение по методам СГ-НЗБ и СГ-±1-НЗБ. Результаты экспериментов по стойкости данных методов к различным методам стегоанализа приведены ниже.

Так, результаты визуального стегоанализа для СГ-НЗБ и СГ-±1-НЗБ при различных долях вложения приведены на рис. 1 и 2, соответственно.

Как видно из рис. 1–2, визуальная атака практически во всех случаях определяет наличие вложенного сообщения при доле вложения более 10%. Как известно [13], визуальная атака не является достоверной и эффективной, и если стегоаналитик наблюдает шумовое поле — такое изображение требует дальнейшего анализа, поскольку нельзя однозначно сказать, что данное изображения имеет вложение, а не является, например, изображением с сильным шумом.

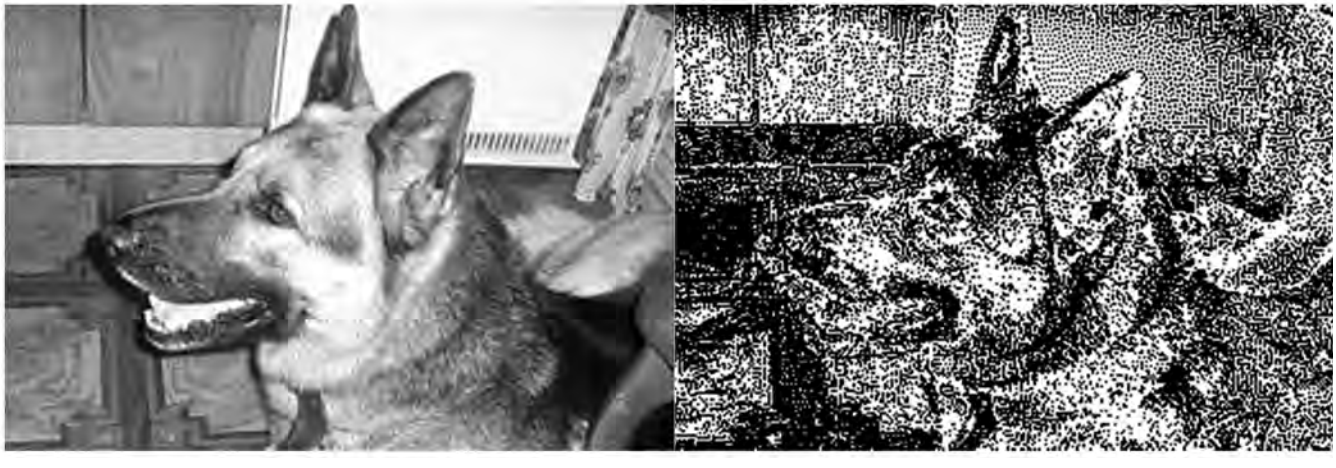

Рис. 1. Изображения с вложением по методу СГ-НЗБ до и после атаки, при долях вложения а) 0%, б) 10%, в) 50%, г) 100%

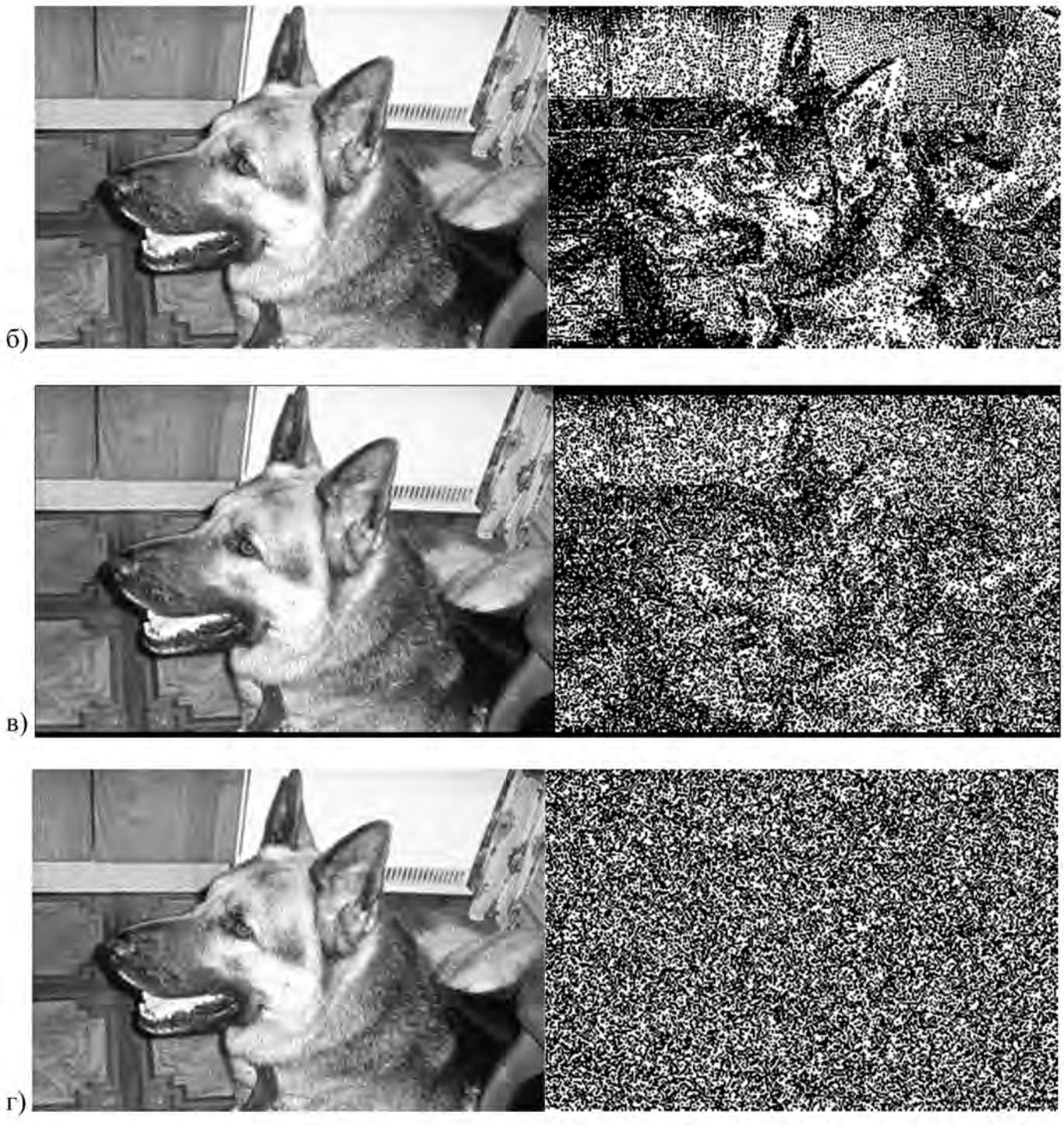

Рис. 1. Изображения с вложением по методу СГ-НЗБ до и после атаки, при долях вложения а) 0%, б) 10%, в) 50%, г) 100%

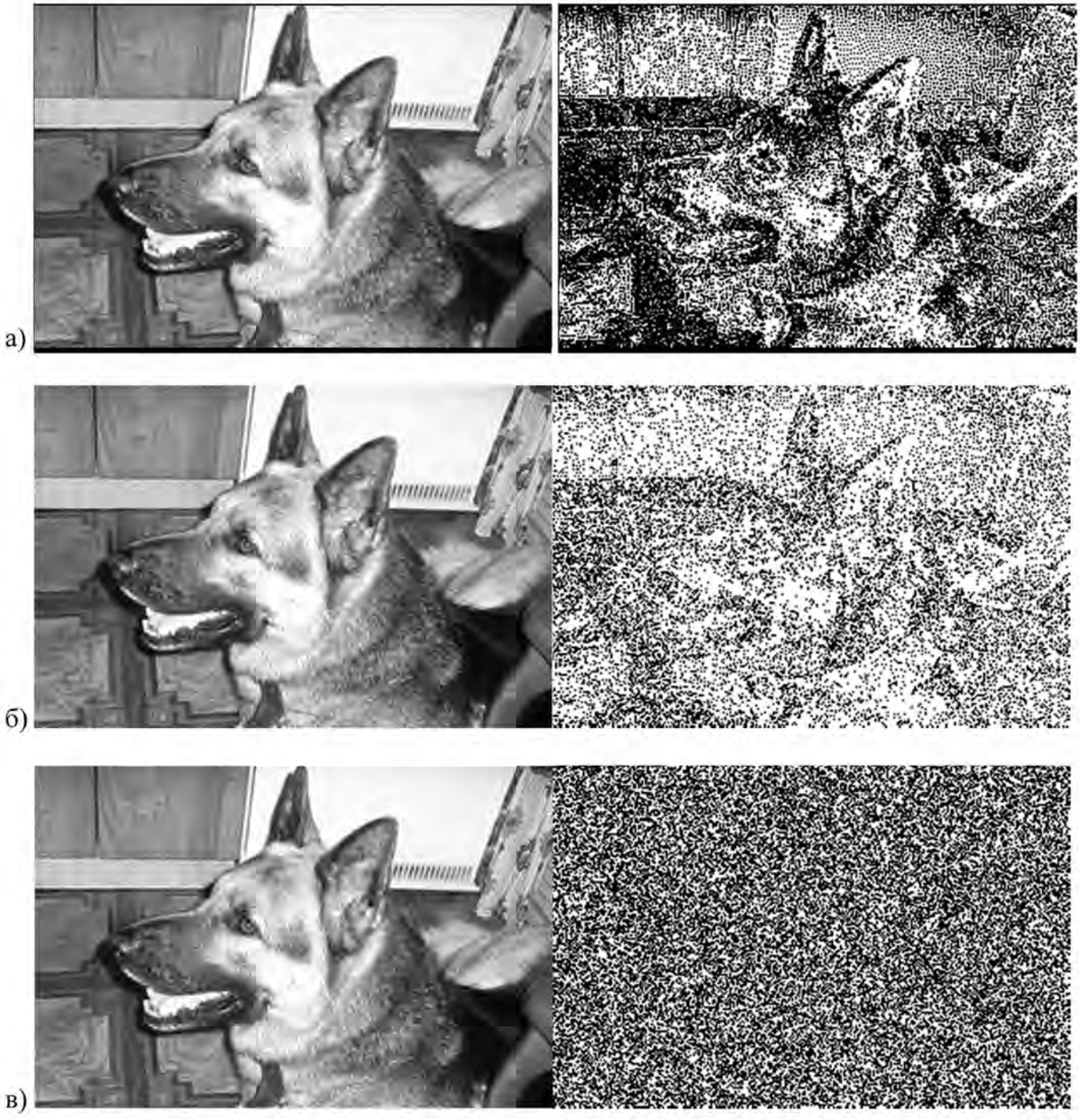

Рис. 2. Изображения с вложением по методу СГ-НЗБ+-1 до и после атаки, при доле вложения а) 10%, б) 50%, в) 100%

И в то же самое время четкость контуров исходного изображения позволяет сделать вывод об отсутствии в данном образце вложения. Так рис. 1б) и 2б), с долей вложения 10%, имеют четкие контуры исходного изображения, и следовательно, логичнее сделать вывод, что в данных исследуемых объектах нет вложения.

Гораздо эффективнее и надежнее выявляют скрытые вложения методы статистического стегоанализа, два из которых будут рассмотрены далее. Для наглядности результаты исследований статистического стегоанализа приведены на графиках, изображенных на рис. 3–8.

Так на рис. 3–5 отображены значения χ^2 покрывающих объектов, а также стеганограмм, созданных с помощью методов СГ-НЗБ и СГ-±1-НЗБ при долях вложения 10%, 50% и 100%, соответственно.

Из графиков, представленных на рис. 3–5 можно сделать вывод, что для СГ-±1-НЗБ данный метод стегоанализа менее эффективный, чем для метода СГ-НЗБ, поскольку во всех 3 случаях график, отображающий распределение СГ-±1-НЗБ, расположен ближе к графику покрывающего объекта, чем график СГ-НЗБ. Также заметим, что для выборок однотипных изображений (с одинаковыми размерами, качеством изображения) возможно выбрать пороговое значение для обнаружения СГ-НЗБ. Для стегосистем с вложением по методу СГ-±1-НЗБ так же возможно выбрать пороговое значение, однако в данном случае эффективность обнаружения будет ниже, чем в случае с СГ-НЗБ, либо неэффективной, что обуславливается симметричным характером вложения СГ-±1-НЗБ.

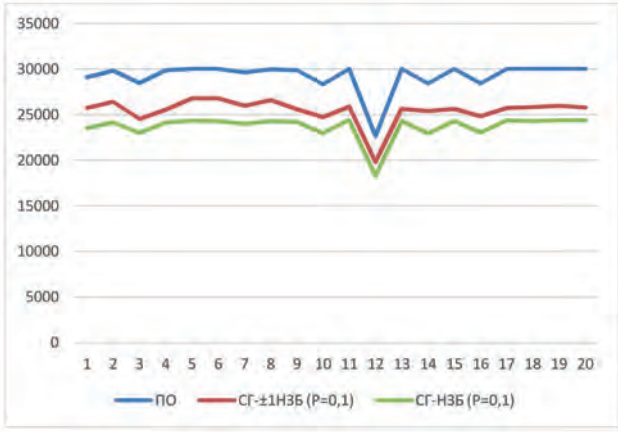

Рис. 3. График распределения значений χ^2 для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 10%

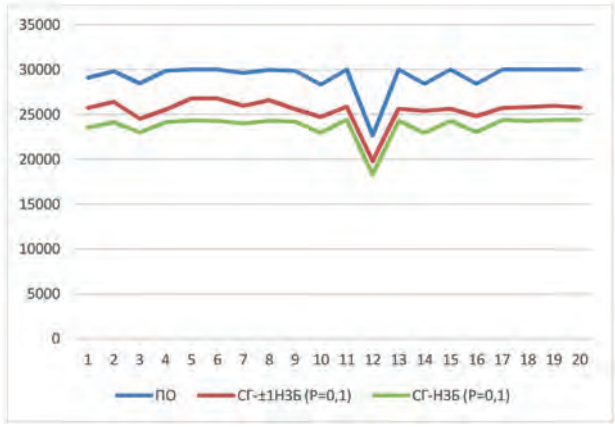

Рис. 5. График распределения значений χ^2 для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 100%

Результаты исследований по методу парно-выборочного анализа выборок покрывающих объектов и соответствующим им стеганограмм, созданным с помощью СГ-НЗБ и СГ-±1-НЗБ представлены на рис. 6–8.

Как видно из графиков, представленных на рис. 6–8, с помощью стегоанализа по методу парно-выборочного

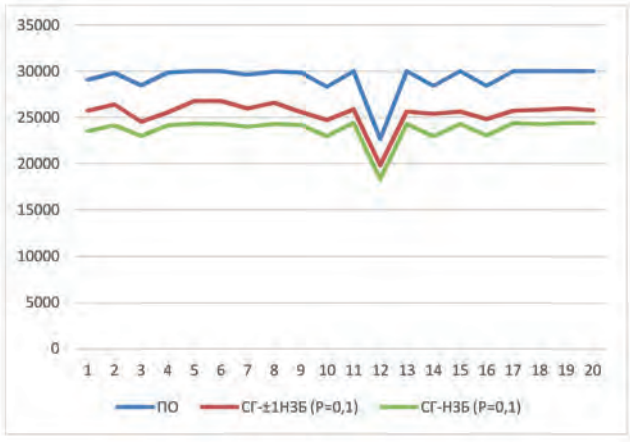

Рис. 4. График распределения значений χ^2 для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 50%

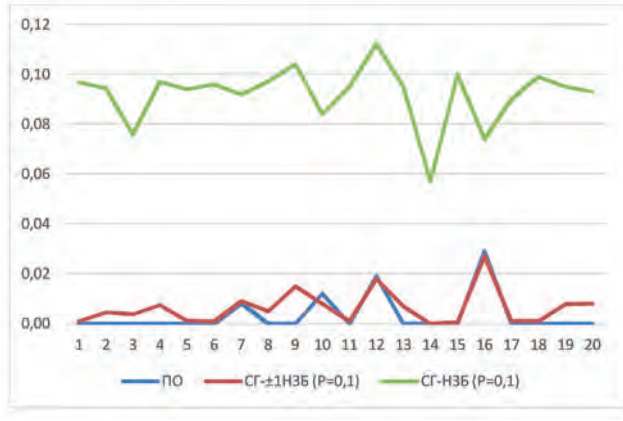

Рис. 6. График распределения значений P' для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 10%

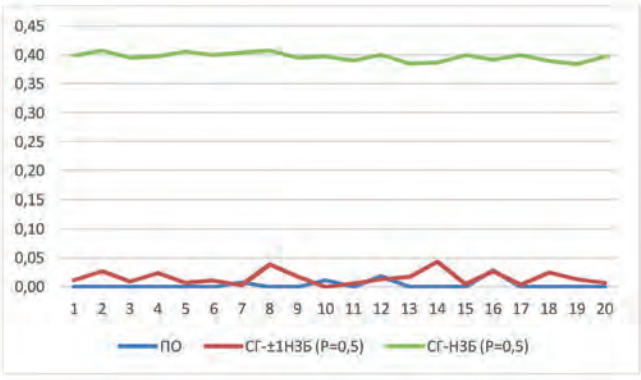

Рис. 7. График распределения значений *P*' для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 50%

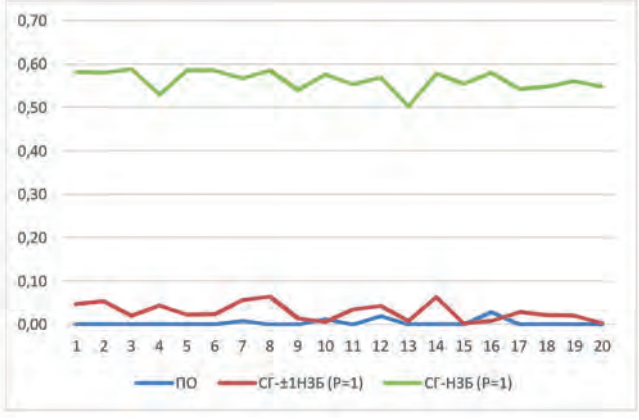

Рис. 8. График распределения значений *P*' для покрывающего объекта; СГ-НЗБ и СГ-±1-НЗБ при доле погружения 100%

анализа не только возможно определить наличие вложения, выполненного по методу СГ-НЗБ, но и выбрать универсальный порог для всех исследуемых объектов, оптимальным пороговым значением по мнению авторов метода является значение 0. Также отметим, что парно-выборочный метод анализа позволяет оценить долю вложенное информации, если доле вложения не более 10%.

При этом, для метода вложения СГ-±1-НЗБ данный вид стегоанализа оказывается неэффективным, поскольку графики покрывающего объекта и СГ-±1-НЗБ, если и не сливаются в одну линию, то пересекаются и идут очень близко на всех 3 графиках. Следовательно, в данном случае рекомендованное авторами метода пороговое значение окажется неэффективным, а самостоятельно выбрать данный порог крайне сложно.

Как показано, метод с замещением достаточно легко обнаруживается с помощью рассмотренных выше методов стегоанализа, поскольку вложение методом СГ-НЗБ носит асимметричный характер. При этом рассмотренные выше методы стегоанализа оказались неэффективны для СГ-±1-НЗБ.

Заключение

Основная идея использования СГ-±1-НЗБ вместо обычного НЗБ-замещения заключается в том, что обычное СГ-НЗБ обладает некоторой несимметрией. Что, в свою очередь, приводит к появлению характерных статистических признаков, позволяющих сделать процедуру обнаружения более надежной. Рандомизация отчетов в процессе вложении дополнительных бит информации позволяет уменьшить изменения статистических свойств гистограммы стеганограммы, и приблизить их к статистический свойствам покрывающего объекта, таким образом данный метод вложения становится более устойчивым к статистическим методам стегоанализа.

Сравнительный анализ стегоатак относительно стегосистем СГ-НЗБ и СГ-±1-НЗБ показал, что:

- СГ-НЗБ не стойка к визуальной атаке с долей вложения более 50%. Модифицированная СГ-НЗБ — СГ-±1-НЗБ так же подвержена визуальной атаке, хотя и более секретна по отношению с СГ-НЗБ за счет симметричного вложения;
- эффективность применения стегоанализа на основе статистики первого порядка относительно СГ-НЗБ выше, чем для СГ-±1-НЗБ.
- СГ-±1-НЗБ стойко к стегоанализу на основе статистики второго порядка, в отличие от СГ-НЗБ, для которого данный вид атаки позволяет не только определить наличие вложения, но и оценить долю вложения, из которой можно рассчитать погруженное количество бит.

На основе материалов, представленных выше, можно сделать вывод, что СГ-±1-НЗБ обеспечивает большую секретность, чем СГ-НЗБ, вследствие чего, если стоит выбор из двух стегосистем, для хранения и передачи дополнительной информации рекомендуется использовать стегосистемы с вложением в наименьший значащий бит с согласованием.

При этом, в дальнейшей работе стоит рассмотреть возможные модификации вложения в наименьшие значащие биты, для повышения стойкости к известным методам стегоанализа. Для стегоаналитиков необходимо модифицировать известные и разработать новые методы стегоанализа для рассмотренных выше стегосистем, для улучшения методов обнаружения.

Литература

1. *Годлевский А. К., Коржик В. И.* Стегосистемы повышенной секретности для вложения информации в неподвижные изображения // Сборник научных статей V международной научно-технической и научно-методической конференции «Актуальные

проблемы инфотелекоммуникаций в науке и образовании». 2016. С. 320–323.

2. *Shterenberg S.I., Krasov A.V., Ushakov I.A.* Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. 2015. Vol. 80. No. 1. С. 28–34.

3. *Герлинг Е.Ю., Ахрамеева К.А.* Обзор современного программного обеспечения, использующего методы стеганографии // Экономика и качество систем связи. 2019. № 3 (13). С. 51–58.

4. *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. Vol. 9. No. 6. Pp. 5218–5226.

5. *Ker A.* Steganalysis of LSB Matching in Grayscale Images // Signal Processing Letters. 2005. Vol. 12. Pp. 441–444.

6. *Luo W., Huang F., Huang Luo J.* Edge Adaptive Image Steganography Based on LSB Matching Revisited // Transactions on Information Forensics and Security. 2010. Vol. 5. Pp. 201–214.

7. *Lee Y.-K., Bell G., Huang S.-Y., Wang R.-Z., Shyu S.-J.* An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding // Lecture Notes in Computer Science. 2009. Vol. 5414. Pp. 349-360.

8. *Korzhik V., 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. Vol. 11. No. 1. Pp. 44–57.

9. *Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G.* Steganalysis Based on Statistical Properties of the Encrypted Messages // In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. LNCS10446. 2017. Pp. 288–298. DOI: 10.1007/978–3–319–65127–9_23

10. *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.

11. *Dumitrescu S., Wu X., Wang Z.* Detection of LSB Steganography via Sample Pair Analysis // IEEE Transactions on Signal Processing. 2003. Vol. 51. No. 7. Pp. 1995–2007. doi: 10.1109/TSP.2003.812753

12. *Dumitrescu S., Wu X., Wang Z.,* Detection of LSB Steganography via Sample Pair Analysis // Information Hiding. IH 2002. Lecture Notes in Computer Science / Petitcolas F.A.P. (eds). Springer, Berlin, Heidelberg, 2003. Vol. 2578. Pp. 355–372.

13. *Герлинг Е.Ю.* Исследование эффективности методов обнаружения стегосистем, использующих вложение в наименее значащие биты // Информационные системы и технологии. 2011. № 4. С. 137–144.

COMPARATIVE ANALYSIS OF STEGOSYSTEMS WITH EMBEDDING IN THE LEAST SIGNIFICANT BITS WITH MATCHING AND SUBSTITUTION

KSENIYA A. AKHRAMEEVA

St-Petersburg, Russia, oklaba@mail.ru

EKATERINA U. GERLING

St-Petersburg, Russia, gerlingeu@gmail.com

KEYWORDS: steganography; embedding in the smallest significant bits; steganalysis; covering object; steganogram.

ABSTRACT

The work presents the results of a comparative analysis of stegosystems with algorithms for embedding in the least significant bit with matching and substitution for differences in the procedure for embedding additional information in the covering object and the resistance of the obtained steganograms to various methods of steganalysis. When using stegosystems with embedding algorithms in the least significant bit with matching and substitution, samples of steganograms with different embedding fractions were obtained for a sample of 200 covering objects. The results of the steganogram analysis on the steganogram data were analyzed, the obtained steganogram samples were compared to the detection of the presence of an additional information attachment using three steganalysis methods: visual attack, first-order statistical attack (chi-square attack) and second-order statistical attack (pairwise selective analysis

attack). The presented example of images before and after a visual attack, for samples steganograms with attachments in the least significant bit with substitution and matching, with an investment fraction of 10%, 50% and 100%, allows to demonstrate the performance of the visual method steganalysis. The graphical representation of the results for first-and second-order attacks allows us to evaluate the effectiveness of the studied methods of stegoanalysis for stegosystems with algorithms for embedding in the least significant bit with matching and substitution. It is shown that a stegosystem with an algorithm for embedding in the least significant bits with matching is more resistant to detection attacks using modern methods of stegoanalysis. Conclusions are made about the possibility of applying the considered methods of stegoanalysis to the presented methods of stegosystems.

REFERENCES

1. Godlevskiy A., Korzhik V. Stegosystem with Improved Security for Embedding of Information Into Digital Motionless Images. *V sborni-ke: Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii sbornik nauchnyh statej V mezhdunarodnoj nauchno-tehnicheskoj i nauchno-metodicheskoj konferencii* [In the collection: Actual problems of infotelecommunications in science and education collection of scientific articles of the V international scientific-technical and scientific-methodical conference] 2016. Pp. 320–323.

2. Shterenberg S.I., Krasov A.V., Ushakov I.A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files. *Journal of Theoretical and Applied Information Technology.* 2015. Vol. 80. No. 1. C. 28–34.

3. Gerling E.U., Ahrameeva K.A. The review of the modern software using sreganography methods. *Jekonomika i kachestvo sistem svjazi* [Economy and quality of communication systems] 2019. No. 3 (13). Pp. 51–58. (In Rus)

4. 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. Vol. 9. No. 6. Pp. 5218–5226.

5. Ker A. Steganalysis of LSB Matching in Grayscale Images. *Signal Processing Letters.* 2005. Vol. 12. Pp. 441–444.

6. Luo W., Huang F., Huang Luo J. Edge Adaptive Image Steganography Based on LSB Matching Revisited. *Transactions on Information Forensics and Security.* 2010. Vol. 5. Pp. 201–214.

7. Lee Y.-K., Bell G., Huang S.-Y., Wang R.-Z., Shyu S.-J. An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding. *Lecture Notes in Computer Science*. 2009. Vol. 5414. Pp. 349-360.

8. Korzhik V., 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. Vol. 11. No. 1. Pp. 44–57.

9. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis Based on Statistical Properties of the Encrypted Messages. *In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security.* LNCS10446. 2017. Pp. 288–298. DOI: 10.1007/978–3–319–65127–9_23

10. Ahrameeva K.A. Gerling E.U., Radynskaya V.E. Automatization for visual steganalysis of LSB. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tehnologii i dizajna. Serija 1. Estestvennye i tehnicheskie nauki* [Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and technical sciences] 2020. No. 1. Pp. 42–45.

11. Dumitrescu S., Wu X., Wang Z. Detection of LSB Steganography via Sample Pair Analysis. *IEEE Transactions on Signal Processing.* 2003. Vol. 51. No. 7. Pp. 1995–2007. doi: 10.1109/TSP.2003.812753

12. Dumitrescu S., Wu X., Wang Z., Detection of LSB Steganography via Sample Pair Analysis. *Information Hiding. IH 2002. Lecture Notes in Computer Science.* By ed. Petitcolas F.A.P. Springer, Berlin, Heidelberg, 2003. Vol. 2578. Pp. 355–372.

13. Gerling, E.U. Investigation of the effectiveness of detection methods stegosystems, which use an embedding to the least significant bits. *Informacionnye sistemy i tehnologii* [Information systems and technologies.] 2011. No. 4. Pp. 137–144. (In Rus)

INFORMATION ABOUT AUTHORS:

Akhrameeva K.A., PhD, Associate Professor at the Department of Secure Communication Systems, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications;

Gerling E.U., PhD, Associate Professor at the Department of Secure Communication Systems, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

For citation: Akhrameeva K.A., Gerling E.U. Comparative analysis of stegosystems with embedding in the least significant bits with matching and substitution. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 38–47. doi: 10.36724/2409-5419-2020-12-6-38-47 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-48-59

ОБОБЩЕННЫЙ СПОСОБ ПРИМЕНЕНИЯ ХЭШ-ФУНКЦИИ ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ

ДИЧЕНКО
Сергей Александрович[1]

ФИНЬКО
Олег Анатольевич[2]

АННОТАЦИЯ

Рассматриваются системы хранения данных, предназначенные для хранения больших многомерных массивов информации, функционирующие в условиях деструктивных воздействий злоумышленника и среды. Одной из актуальнейших для подобных систем задач является организация безопасного хранения данных, а с учетом таких условий функционирования – обеспечение их целостности. Обеспечение целостности данных является сложной задачей, ввиду своей комплексности, так как включает в себя и восстановление, и контроль целостности данных. Одним из известных и широко используемых способов контроля целостности данных является применение криптографических методов, в частности, функции хэширования. Однако, несмотря на повсеместное применение хэш-функций, они крайне мало исследованы, а практические предложения по их применению весьма немногочисленны и характеризуются рядом недостатков, связанных, с необходимостью введения высокой избыточности контрольной информации. В условиях ограничения на существующий ресурс систем хранения данных это может привести к снижению вероятности выполнения задачи их функционирования или вообще к ее невыполнению. Предложен обобщенный способ, применение которого позволит снизить объем вводимой избыточности при контроле целостности информации в системах хранения данных, основанный на применении криптографических хэш-функций, отличительной особенностью которого является использование правилах построения помехоустойчивых кодов. К тому же, разработанный способ обеспечивает процедуру контроля целостности данных новым свойством: возможностью осуществления контроля целостности не только данных, подлежащих защите, но и самих эталонных хэш-кодов. Получены расчетные данные требуемого объема вводимой избыточности при контроле целостности данных в существующих системах хранения при использовании разработанного способа.

Сведения об авторах:

[1]к.т.н., докторант Краснодарского высшего военного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия, dichenko.sa@yandex.ru

[2]д.т.н., профессор, профессор Краснодарского высшего военного училища имени генерала армии С.М. Штеменко; профессор Северо-Кавказского федерального университета; академический советник Российской академии ракетных и артиллерийских наук (РАРАН), г. Краснодар, Россия, ofinko@yandex.ru; www.mathnet.ru/person40004

КЛЮЧЕВЫЕ СЛОВА: система хранения данных; контроль целостности данных; криптографические методы; хэш-функция; снижение вводимой избыточности.

Для цитирования: *Диченко С.А., Финько О.А.* Обобщенный способ применения хэш-функции для контроля целостности данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. №6. С. 48–59. doi: 10.36724/2409-5419-2020-12-6-48-59

Введение

Системы хранения данных (СХД) являются одним из основных сегментов информационных систем (ИС) различного назначения. В современных условиях увеличения объема и ценности обрабатываемой информации при проектировании и разработке новых СХД возникает задача нахождения оптимального решения для контроля и восстановления целостности хранящейся в них информации [1, 2].

Особую актуальность разработка СХД с оптимальными решениями для контроля и восстановления целостности данных приобретает при ограничениях на их ресурсы. В этом случае объем вводимой для контроля и восстановления целостности данных избыточности будет иметь большое значение при обеспечении устойчивости ИС в процессе их целевого функционирования. Многократное резервирование данных и вычисление эталонной контрольной информации при контроле целостности данных после каждого восстановления, может привести к полному израсходованию ресурсов СХД, наступление которого приведет к снижению вероятности выполнения задачи их функционирования или вообще к ее невыполнению[1] [3].

Актуальность исследований в области снижения вводимой избыточности при контроле и восстановлении целостности информации в современных СХД подтверждается Стратегией развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года[2], где одной из основных задач государства по развитию отрасли информационных технологий в этом направлении является развитие центров обработки и хранения информации как материальной основы для обработки и хранения больших массивов данных.

Анализ существующих способов контроля целостности данных

Известны различные способы применения хэш-функции для контроля целостности данных, подлежащих защите[3]. На рис. 1 представлена классификация способов применения хэш-функции к данным, выполненная в зависимости от состава и порядка вычисления эталонных хэш-кодов.

1. Способ применения хэш-функции h для k блоков данных, представленных двоичными векторами $\mathbf{M}_i (i = 1, 2, \ldots, k)$, с вычислением одного общего хэш-кода $\mathbf{H}$:

$$h(\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_k) = \mathbf{H}$$

поясняется на рис. 2.

Достоинство: низкая избыточность.

Недостатки:

– отсутствие возможности локализации блока данных, представленного двоичным вектором $\mathbf{M}_i$, при контроле целостности данных;

– малая вероятность обнаружения ошибки (определения факта нарушения целостности данных) при пропуске ошибки (ложном сигнале об ошибке) средствами контроля.

[1]Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006. 504 с.

[2]Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года (утв. распоряжением Правительства РФ от 1 ноября 2013 г. N 2036-р).

[3]Schneier B. Applied Cryptography Second Edition: protocols, algorithms and source code in C. John Wiley & Sons, Inc. 2016. 653 p.

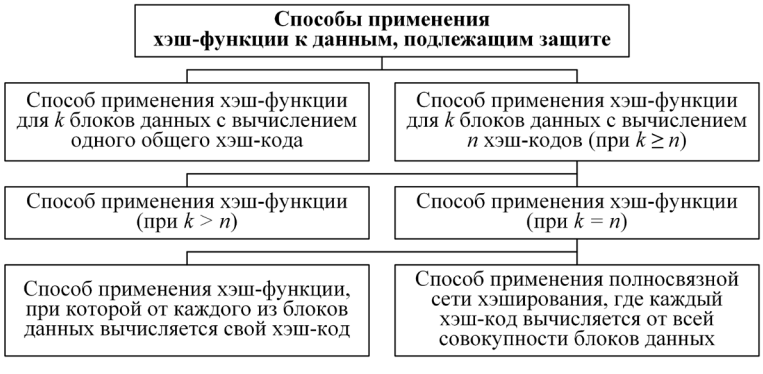

Рис. 1. Классификация способов применения хэш-функции к данным

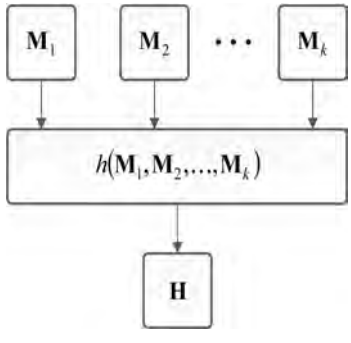

Рис. 2. Способ применения хэш-функции для k блоков с вычислением общего хэш-кода

2. Способы применения хэш-функции для k блоков данных с вычислением n хэш-кодов (при $k \geq n$) подразделяются на:

2.1. Способы применения хэш-функции (при $k = n$), которые в свою очередь можно разделить на:

а) способ применения хэш-функции, при котором от каждого из блоков данных, представленных двоичными векторами $\mathbf{M}_i$, вычисляется свой хэш-код $\mathbf{H}_i$;

б) способ применения полносвязной сети хэширования, при котором каждый хэш-код $\mathbf{H}_i$ вычисляется от всей совокупности данных, представленных двоичными векторами $\mathbf{M}_i$;

2.2. Способы применения хэш-функции (при $k \geq n$).

Способ применения хэш-функции h, при котором от каждого из блоков данных, представленных двоичными векторами $\mathbf{M}_i$, вычисляется хэш-код $\mathbf{H}_i$:

$$h(\mathbf{M}_i) = \mathbf{H}_i$$

поясняется на рис. 3.

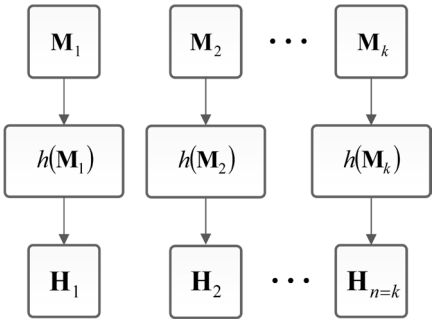

Рис. 3. Способ применения хэш-функции, при которой от каждого из блоков данных вычисляется хэш-код

В этом случае, количество вычисленных хэш-кодов $\mathbf{H}_i$ будет равняться количеству двоичных векторов $\mathbf{M}_i$.

Достоинства:

– простота реализации;

– возможность локализации блока данных, представленного двоичным вектором $\mathbf{M}_i$, при контроле целостности данных.

Недостатки:

– высокая избыточность при контроле целостности блоков данных, представленных двоичными векторами небольшой размерности;

– малая вероятность обнаружения ошибки (определения факта нарушения целостности данных) при пропуске ошибки (ложном сигнале об ошибке) средствами контроля.

Способ применения полносвязной сети хэширования, при котором каждый хэш-код $\mathbf{H}_i$ вычисляется от всей совокупности данных, представленных двоичными векторами $\mathbf{M}_i$:

$$h\left(\mathbf{M}_{j_1} \| \mathbf{M}_{j_2} \| \ldots \| \mathbf{M}_{j_k}\right) = \mathbf{H}_i$$

поясняется на рис. 4.

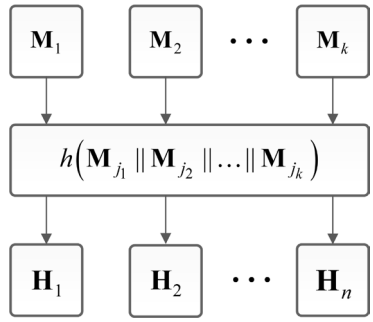

Рис. 4. Способ применения полносвязной сети хэширования

В данном способе большое значение имеет последовательность блоков данных, представленных двоичными векторами $\mathbf{M}_i$, участвующих в конкатенации (объединении). Здесь первым объединяется блок данных, представленный двоичными векторами $\mathbf{M}_i$, номер которого соответствует номеру вычисляемого хэш-кода $\mathbf{H}_i$ (за счет этого их значения будут отличаться между собой).

Например,

– при $i = 1: \mathbf{H}_1 = h\left(\mathbf{M}_1 \| \mathbf{M}_2 \| \ldots \| \mathbf{M}_k\right)$;

– при $i = 2: \mathbf{H}_2 = h\left(\mathbf{M}_2 \| \mathbf{M}_1 \| \mathbf{M}_3 \| \ldots \| \mathbf{M}_k\right)$;

– при $i = k: \mathbf{H}_n = h\left(\mathbf{M}_n \| \ldots \| \mathbf{M}_{n-1} \| \mathbf{M}_{n+1} \| \ldots \| \mathbf{M}_k\right)$,

где «||» — операция конкатенации.

Достоинство: повышение вероятности обнаружения ошибки (определения факта нарушения целостности данных) при пропуске ошибки (ложном сигнале об ошибке) средствами контроля.

Недостатки:

– высокая избыточность при контроле целостности блоков данных, представленных двоичными векторами небольшой размерности;

– в общем виде данная схема не позволяет выполнить локализацию блока данных в случае нарушения его целостности.

Однако, частные случаи способа применения функции хэширования (рис. 4) позволяют локализовать блок данных с нарушением целостности с одновременным снижением вводимой избыточности, в отличие от способов, представленных на рис. 2 и 3.

В свою очередь, при контроле целостности данных наибольший интерес представляют способы применения хэш-функции (при $k>n$). В [4, 5] представлено решение, позволяющее обеспечить локализацию искаженных или утраченных блоков данных, подлежащих защите, с одновременным снижением избыточности контрольной информации при осуществлении контроля целостности данных в автоматизированных системах, где с помощью математического аппарата теории систем векторов выполнено обоснование и разработка алгоритма построения линейных систем хэш-кодов, правила (принципы) построения которых аналогичны правилам построения линейных избыточных кодов, в частности, кодов Хемминга.

Известны другие способы применения хэш-функции, позволяющие локализовать блоки данных, с нарушенной целостностью с одновременным снижением вводимой избыточности[4] [6–8]. Главными недостатками представленных способов являются: отсутствие возможности определения факта нарушения целостности данных в условиях искажения или уничтожения самой контрольной информации, что может привести к пропуску ошибки или ложном сигнале об ошибке; а также они не учитывают структуру многомерного представления информации в современных СХД.

Разработка способа

Способ снижения вводимой избыточности при контроле целостности данных, представленных в СХД в виде упорядоченных многомерных массивов (гиперкубов), основан на правилах построения помехоустойчивых кодов.

Путем фиксации одного из измерений гиперкуба данных сформируем матрицу $\mathbf{W}$, на строках и столбцах которой располагаются подблоки данных $\mathbf{M}_{ij}$, подлежащие защите [9–11]:

$$\mathbf{W} = \begin{bmatrix} \mathbf{M}_{11} & \mathbf{M}_{12} & \cdots & \mathbf{M}_{1k} \\ \mathbf{M}_{21} & \mathbf{M}_{22} & \cdots & \mathbf{M}_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{M}_{n1} & \mathbf{M}_{n2} & \cdots & \mathbf{M}_{nk} \end{bmatrix}. \quad (1)$$

При этом строки матрицы (1) образуют блоки данных $\mathbf{M}_i = \{\mathbf{M}_{i1} \| \mathbf{M}_{i2} \| \dots \| \mathbf{M}_{in}\}$, где i=1,2, …, k; а столбцы матрицы (1) образуют блоки данных $\mathbf{M}_j = \{\mathbf{M}_{1j} \| \mathbf{M}_{2j} \| \dots \| \mathbf{M}_{kj}\}$, где j = 1,2, …, n.

Для контроля целостности подблоков данных $\mathbf{M}_{ij}$ применим хэш-функцию по правилам построения прямоугольных, квадратных, треугольных, кубических кодов[5].

Использование полученных конструкций при контроле целостности данных позволит снизить избыточность контрольной информации. При этом оценивание количества вводимой избыточности (контрольной информации) будет производиться в соответствии с выражением:

$$V = \frac{p}{d}, \quad (2)$$

где V — объем вводимой избыточности, d — количество подблоков данных, подлежащих защите, p — количество вычисляемых хэш-кодов.

Контроль целостности данных на основе правил построения прямоугольных кодов

Контроль целостности данных, основанный на правилах построения прямоугольных кодов, содержит ($k \cdot n$) блоков данных (здесь и далее символический смысл k, n переопределен), представленных двоичными векторами $\mathbf{M}_{ij} (i = 1,\dots,n\,;\, j = 1,\dots,k)$, которые представляются в прямоугольнике размером k на n (распределяются по k столбцам и n строкам прямоугольника).

По правилам построения к каждой строке и столбцу прямоугольника добавляются хэш-коды $\mathbf{H}_{i,k+1}$, $\mathbf{H}_{n+1,k}$, которые вычисляется от совокупности блоков данных, представленных двоичными векторами $\mathbf{M}_{ij}$, расположенных на соответствующей строке и столбце прямоугольника, как представлено на рис. 5.

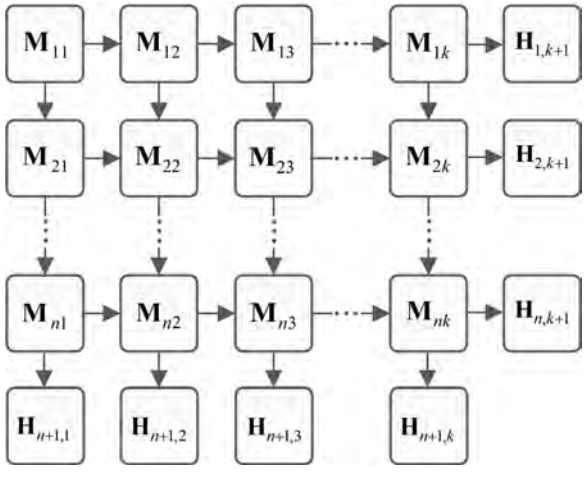

Рис. 5. Общий вид прямоугольной системы хэш-кодов

[4]Knuth D.E. The Art of Computer Programming: Volume 3: Sorting and Searching. 2nd edn. 2018. 803 p.

[5]Hamming R. Coding and Information Theory. Prentice-Hall, 2008. 259 p.

При этом матрица (1) примет следующую форму:

$$\Psi = \left[\begin{array}{cccc|c} \mathbf{M}_{11} & \mathbf{M}_{12} & \dots & \mathbf{M}_{1k} & \mathbf{H}_{1,k+1} \\ \mathbf{M}_{21} & \mathbf{M}_{22} & \dots & \mathbf{M}_{2k} & \mathbf{H}_{2,k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{M}_{n1} & \mathbf{M}_{n2} & \dots & \mathbf{M}_{nk} & \mathbf{H}_{n,k+1} \\ \hline \mathbf{H}_{n+1,1} & \mathbf{H}_{n+1,2} & \dots & \mathbf{H}_{n+1,k} & \end{array}\right].$$

Определение 1. Первоначальный прямоугольник размером k на n подблока данных преобразуется в массив размером $((k+1)\cdot(n+1)-1)$, который будет называться *прямоугольной системой хэш-кодов*.

Для контроля целостности $(k\times n)$ блоков данных в прямоугольной системе хэш-кодов требуется вычислить $(k\times n)$ хэш-кодов.

В соответствии с (2) объем вводимой избыточности вычисляется по формуле:

$$V = \frac{k+n}{k\cdot n}. \qquad (3)$$

Контроль целостности, а также локализация блока данных в случае нарушения его целостности осуществляется при построении сети хэширования.

Сеть хэширования для прямоугольной системы хэш-кодов, представленной на рис. 6.

Пример 1. Сеть хэширования для прямоугольной системы хэш-кодов с размером прямоугольника ($k=3$, $n=2$) представлена на рис. 7.

На основе сети хэширования (рис. 7) составляется табл. 1, где «[•]» обозначает локализованный проверяемый хэш-код $\tilde{\mathbf{H}}_{i,k+1}$ или $\tilde{\mathbf{H}}_{n+1,k}$, а также при нарушении целостности данных проверяемый блок данных $\tilde{\mathbf{M}}_{i,j}$

На основе полученного синдрома принимается решение об искаженном или утраченном подблоке данных, подлежащих защите.

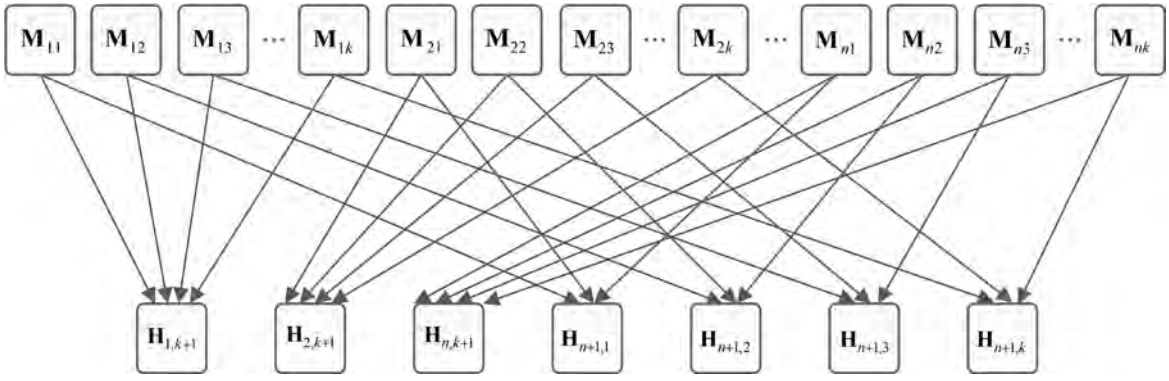

Рис. 6. Общий вид сети хэширования для прямоугольной системы хэш-кодов

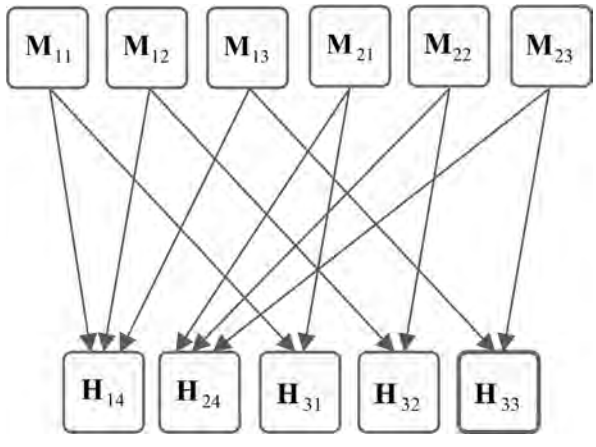

Рис. 7. Сеть хэширования для прямоугольной системы хэш-кодов, где k=3, n=2

Таблица 1

Синдромы для прямоугольной системы хэш-кодов, где $k = 3$, $n = 2$

Синдром					Локализация ошибки
$\mathbf{H}_{33}$	$\mathbf{H}_{32}$	$\mathbf{H}_{31}$	$\mathbf{H}_{24}$	$\mathbf{H}_{14}$	Результат
0	0	0	0	0	Нет ошибки
0	0	0	0	1	$\left[\tilde{\mathbf{H}}_{14}\right], \mathbf{H}_{24}, \mathbf{H}_{31}, \mathbf{H}_{32}, \mathbf{H}_{33}, \mathbf{M}_{11}, \ldots, \mathbf{M}_{23}$
0	0	0	1	0	$\mathbf{H}_{14}, \left[\tilde{\mathbf{H}}_{24}\right], \mathbf{H}_{31}, \mathbf{H}_{32}, \mathbf{H}_{33}, \mathbf{M}_{11}, \ldots, \mathbf{M}_{23}$
0	0	1	0	0	$\mathbf{H}_{14}, \mathbf{H}_{24}, \left[\tilde{\mathbf{H}}_{31}\right], \mathbf{H}_{32}, \mathbf{H}_{33}, \mathbf{M}_{11}, \ldots, \mathbf{M}_{23}$
0	1	0	0	0	$\mathbf{H}_{14}, \mathbf{H}_{24}, \mathbf{H}_{31}, \left[\tilde{\mathbf{H}}_{32}\right], \mathbf{H}_{33}, \mathbf{M}_{11}, \ldots, \mathbf{M}_{23}$
1	0	0	0	0	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{32}, \left[\tilde{\mathbf{H}}_{33}\right], \mathbf{M}_{11}, \ldots, \mathbf{M}_{23}$
0	0	1	0	1	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{33}, \left[\tilde{\mathbf{M}}_{11}\right], \mathbf{M}_{12}, \ldots, \mathbf{M}_{23}$
0	1	0	0	1	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{33}, \mathbf{M}_{11}, \left[\tilde{\mathbf{M}}_{12}\right], \mathbf{M}_{13}, \ldots, \mathbf{M}_{23}$
1	0	0	0	1	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{33}, \mathbf{M}_{11}, \mathbf{M}_{12}, \left[\tilde{\mathbf{M}}_{13}\right], \mathbf{M}_{21}, \mathbf{M}_{22}, \mathbf{M}_{23}$
0	0	1	1	0	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{33}, \mathbf{M}_{11}, \mathbf{M}_{12}, \mathbf{M}_{13}, \left[\tilde{\mathbf{M}}_{21}\right], \mathbf{M}_{22}, \mathbf{M}_{23}$
0	1	0	1	0	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{33}, \mathbf{M}_{11}, \ldots, \mathbf{M}_{21}, \left[\tilde{\mathbf{M}}_{22}\right], \mathbf{M}_{23}$
1	0	0	1	0	$\mathbf{H}_{14}, \ldots, \mathbf{H}_{33}, \mathbf{M}_{11}, \ldots, \mathbf{M}_{22}, \left[\tilde{\mathbf{M}}_{23}\right]$

При этом существует возможность осуществления контроля целостности самих эталонных хэш-кодов. Для этого необходимо в соответствии со следующим выражением вычислить хэш-код $\mathbf{H}_{n+1,k+1}$:

$$\mathbf{H}_{n+1,k+1} = h\left(\mathbf{H}_{1,k+1}, \ldots, \mathbf{H}_{n,k+1}, \mathbf{H}_{n+1,k}, \ldots, \mathbf{H}_{n+1,k}\right),$$

расположенный в прямоугольной системе хэш-кодов, как представлено на рис. 8.

При этом матрица (1) примет следующую форму:

$$\mathbf{\Psi} = \left[\begin{array}{cccc|c} \mathbf{M}_{11} & \mathbf{M}_{12} & \ldots & \mathbf{M}_{1k} & \mathbf{H}_{1,k+1} \\ \mathbf{M}_{21} & \mathbf{M}_{22} & \ldots & \mathbf{M}_{2k} & \mathbf{H}_{2,k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{M}_{n1} & \mathbf{M}_{n2} & \ldots & \mathbf{M}_{nk} & \mathbf{H}_{n,k+1} \\ \hline \mathbf{H}_{n+1,1} & \mathbf{H}_{n+1,2} & \ldots & \mathbf{H}_{n+1,k} & \mathbf{H}_{n+1,k+1} \end{array}\right].$$

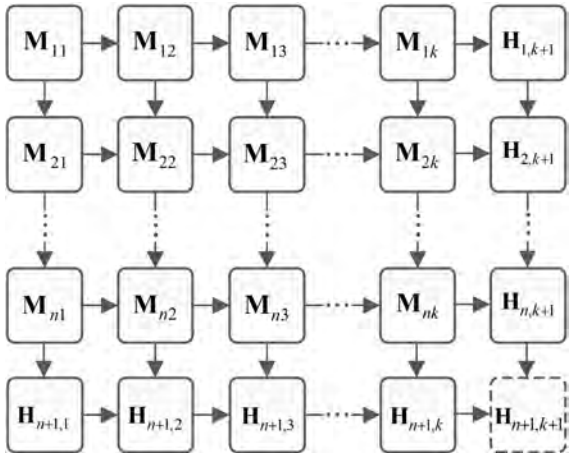

Рис. 8. Прямоугольная система с контролем эталонных хэш-кодов

Определение 2. Хэш-коды, предназначенные для контроля целостности эталонных хэш-кодов, изначально вычисленных для осуществления контроля целостности данных, будут называться *эталонными хэш-кодами второго порядка*.

Контроль целостности данных на основе правил построения квадратных кодов

Квадратная система хэш-кодов является частным случаем прямоугольной системы хэш-кодов (рис. 9). Известно, что при заданном размере $((k+1)\cdot(n+1)-1)$ избыточность тем меньше, чем ближе прямоугольник к квадрату[6].

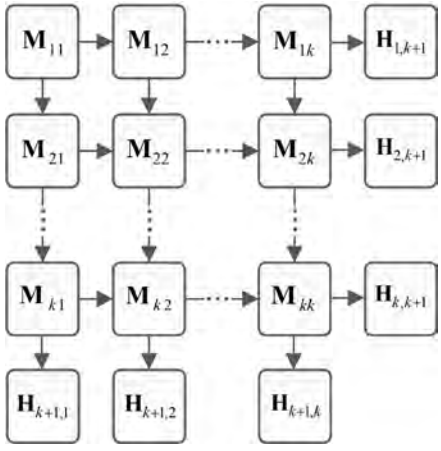

Рис. 9. Общий вид квадратной системы хэш-кодов

При этом матрица (1) примет следующую форму:

$$\Psi = \left[\begin{array}{cccc|c} \mathbf{M}_{11} & \mathbf{M}_{12} & \dots & \mathbf{M}_{1k} & \mathbf{H}_{1,k+1} \\ \mathbf{M}_{21} & \mathbf{M}_{22} & \dots & \mathbf{M}_{2k} & \mathbf{H}_{2,k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{M}_{k1} & \mathbf{M}_{k2} & \dots & \mathbf{M}_{kk} & \mathbf{H}_{k,k+1} \\ \hline \mathbf{H}_{k+1,1} & \mathbf{H}_{k+1,2} & \dots & \mathbf{H}_{k+1,k} & \end{array}\right].$$

Определение 3. *Квадратной системой хэш-кодов* будет называться система хэш-кодов размером $((k+1)^2-1)$, из которых k^2 блоков данных, подлежащих защите, и $2k$ хэш-кодов, расположенных вдоль сторон квадрата.

Для контроля целостности k^2 блоков данных в квадратной системе хэш-кодов требуется вычислить $2k$ хэш-кодов, в соответствии с (2) объем вводимой избыточности вычисляется по формуле:

$$V = \frac{2}{k}. \qquad (4)$$

[4]Hamming R. Coding and Information Theory. Prentice-Hall, 2008. 259 p.

Пример 2. При фиксированном числе подблоков данных, подлежащих защите, к примеру, 144, объем вводимой избыточности в квадратной системе хэш-кодов, где $k = 12$, в соответствии с (4) составит $V \approx 16{,}7\%$, а в прямоугольной системе, где $k = 16$, $n = 9$, в соответствии с (3) составит $V \approx 17{,}4\%$.

Выигрыш при использовании квадратной системы хэш-кодов по сравнению с прямоугольной при количестве подблоков данных равном 144 составит ≈ 4,2%.

Для контроля целостности эталонных хэш-кодов необходимо по аналогии с контролем целостности данных на основе схемы построения прямоугольных кодов вычислить эталонный хэш-код второго порядка.

Контроль целостности данных на основе правил построения треугольных кодов

Определение 4. *Треугольной системой хэш-кодов* будет называться система хэш-кодов размером $\left(\frac{k(k+1)}{2}+k+1\right)$, где для k подблоков данных, подлежащих защите, на соответствующей строке и соответствующем столбце вычисляется хэш-код, как представлено на рис. 10.

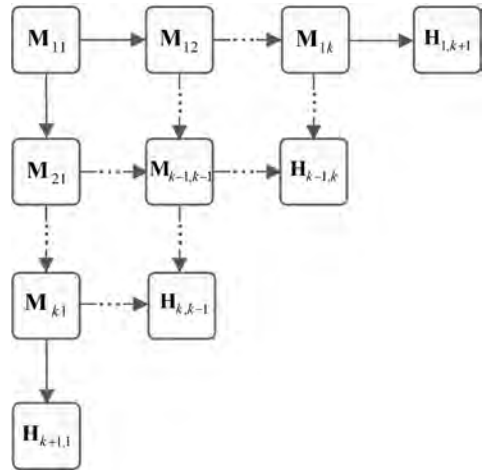

Рис. 10. Общий вид треугольной системы хэш-кодов

При этом матрица (1) примет форму полураспавшейся (клеточно-треугольной) матрицы:

$$\Psi = \left[\begin{array}{ccccc|c} \mathbf{M}_{11} & & \mathbf{M}_{12} & \dots & \mathbf{M}_{1k} & \mathbf{H}_{1,k+1} \\ & \ddots & \vdots & \iddots & & \vdots \\ \mathbf{M}_{21} & \dots & \mathbf{M}_{k-1,k-1} & & & \mathbf{H}_{k-1,k} \\ \vdots & \iddots & & & & \\ \mathbf{M}_{k1} & & & & & \\ \hline \mathbf{H}_{k+1,1} & \dots & \mathbf{H}_{k,k-1} & & & \end{array}\right],$$

Понятие «полураспавшаяся» («клеточно-треугольная») приведены по аналогии, представленной

в работе[7], где клеточная матрица называется *полураспавшейся* или *клеточно-треугольной*, если все ее диагональные клетки — квадратные, а клетки, стоящие по какую-либо одну сторону от главной диагонали, заполнены нулями.

Для контроля целостности $\frac{k(k+1)}{2}$ блоков данных в треугольной системой хэш-кодов требуется вычислить $(k+1)$ хэш-кодов, в соответствии с (2) объем вводимой избыточности вычисляется по формуле:

$$V = \frac{2}{k}. \qquad (5)$$

Для контроля целостности эталонных хэш-кодов необходимо вычислить эталонный хэш-код второго порядка $\mathbf{H}_{k+1,k+1}$:

$$\mathbf{H}_{k+1,k+1} = h\left(\mathbf{H}_{1,k+1},\ldots,\mathbf{H}_{k-1,k},\mathbf{H}_{k+1,1},\ldots,\mathbf{H}_{k,k-1}\right),$$

как представлено на рис. 11.

Для осуществления контроля целостности строится сеть хэширования.

Пример 3. Сеть хэширования для треугольной системы хэш-кодов ($k=3$) представлена на рис. 12.

На основе сети хэширования (рис. 12) составляется табл. 2.

[7] *Мальцев А.И.* Основы линейной алгебры. М.: Государственное издательство технико-теоретической литературы, 1956. 340 с.

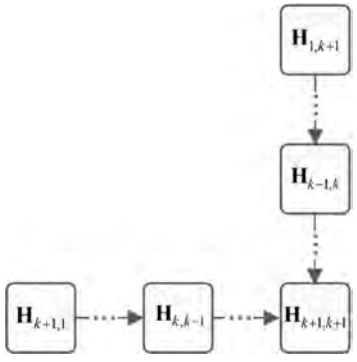

Рис. 11. Контроль эталонных хэш-кодов в треугольной системе

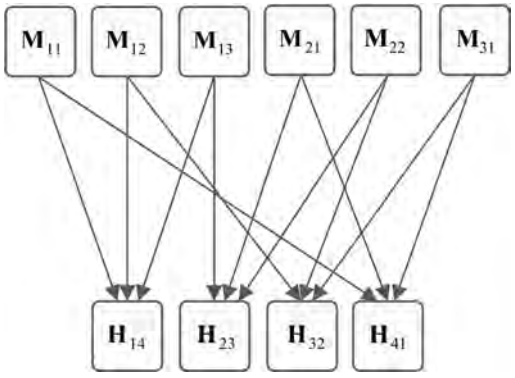

Рис. 12. Сеть хэширования для треугольной системы хэш-кодов, где $k=3$

Таблица 2

Синдромы для треугольной системы хэш-кодов, где $k=3$

Синдром				Локализация ошибки
$\mathbf{H}_{41}$	$\mathbf{H}_{32}$	$\mathbf{H}_{23}$	$\mathbf{H}_{14}$	Результат
0	0	0	0	Нет ошибки
0	0	0	1	$\left[\tilde{\mathbf{H}}_{14}\right],\mathbf{H}_{23},\mathbf{H}_{32},\mathbf{H}_{41},\mathbf{M}_{11},\ldots,\mathbf{M}_{31}$
0	0	1	0	$\mathbf{H}_{14},\left[\tilde{\mathbf{H}}_{23}\right],\mathbf{H}_{32},\mathbf{H}_{41},\mathbf{M}_{11},\ldots,\mathbf{M}_{31}$
0	1	0	0	$\mathbf{H}_{14},\mathbf{H}_{23},\left[\tilde{\mathbf{H}}_{32}\right],\mathbf{H}_{41},\mathbf{M}_{11},\ldots,\mathbf{M}_{31}$
1	0	0	0	$\mathbf{H}_{14},\mathbf{H}_{23},\mathbf{H}_{32},\left[\tilde{\mathbf{H}}_{41}\right],\mathbf{M}_{11},\ldots,\mathbf{M}_{31}$
1	0	0	1	$\mathbf{H}_{14},\ldots,\mathbf{H}_{41},\left[\tilde{\mathbf{M}}_{11}\right],\mathbf{M}_{12},\ldots,\mathbf{M}_{31}$
0	1	0	1	$\mathbf{H}_{14},\ldots,\mathbf{H}_{41},\mathbf{M}_{11},\left[\tilde{\mathbf{M}}_{12}\right],\mathbf{M}_{13},\ldots,\mathbf{M}_{31}$
0	0	1	1	$\mathbf{H}_{14},\ldots,\mathbf{H}_{41},\mathbf{M}_{11},\mathbf{M}_{12},\left[\tilde{\mathbf{M}}_{13}\right],\mathbf{M}_{21},\mathbf{M}_{22},\mathbf{M}_{31}$
1	0	1	0	$\mathbf{H}_{14},\ldots,\mathbf{H}_{41},\mathbf{M}_{11},\mathbf{M}_{12},\mathbf{M}_{13},\left[\tilde{\mathbf{M}}_{21}\right],\mathbf{M}_{22},\mathbf{M}_{31}$
0	1	1	0	$\mathbf{H}_{14},\ldots,\mathbf{H}_{41},\mathbf{M}_{11},\ldots,\mathbf{M}_{21},\left[\tilde{\mathbf{M}}_{22}\right],\mathbf{M}_{31}$
1	1	0	0	$\mathbf{H}_{14},\ldots,\mathbf{H}_{41},\mathbf{M}_{11},\ldots,\mathbf{M}_{22},\left[\tilde{\mathbf{M}}_{31}\right]$

На основе полученного синдрома принимается решение об искаженном или утраченном подблоке данных, подлежащих защите.

Контроль целостности данных на основе правил построения кубических кодов

Схема применения хэш-функции к блокам данных, построенная по правилам, аналогичным правилам построения многомерных структурах, в частности, для трехмерной структуры (куба) содержит $k(k+1)^2$ подблоков данных $\mathbf{M}_{ij}$, подлежащих защите ($i=1,\ldots,\ k+1;\ j=1,\ldots,\ k(k+1)^2$), которые представляются в кубе размером $(k+1)^3$.

Для контроля целостности $k(k+1)^2$ блоков данных в трехмерной системе хэш-кодов требуется вычислить $(k+1)^2$ хэш-кодов, в соответствии с (2) объем вводимой избыточности вычисляется по формуле:

$$V=\frac{1}{k}. \qquad (6)$$

Определение 5. *Трехмерной системой хэш-кодов* будет называться система хэш-кодов размером $(k+1)^3$, где для подблоков данных на соответствующей плоскости вычисляются хэш-коды, как представлено на рис. 13 (частный случай: при $k=2$).

Кроме сокращения вводимой избыточности контрольной информации представленной конструкции присущи отличительные свойства, связанные с увеличением кратности гарантировано обнаруживаемых и локализуемых подблоков данных в случае нарушения их целостности.

Оценивание разработанного способа

Объем вводимой избыточности контрольной информации для контроля целостности данных при использовании разработанного способа в соответствии с выражениями (3)-(6) сокращается со 100% (при использовании существующих решений) до ≈8% в зависимости от количества подблоков данных, подлежащих защите. Снижение

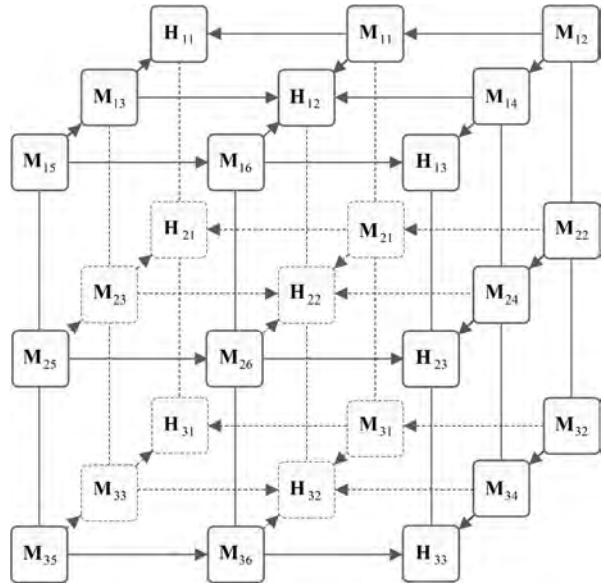

Рис. 13. Общий вид трехмерной системы хэш-кодов, где $k=2$

вводимой избыточности обеспечивается за счет разработанных систем хэш-кодов, при которых требуется меньшее количество хэш-кодов для контроля целостности подблоков данных, подлежащих защите, по сравнению с существующими решениями.

Для демонстрации полученного выигрыша выполним оценивание каждой разработанной системы хэш-кодов. Для этого составим табл. 3, где при фиксированном значении переменной k в представленных системах количество подблоков данных, подлежащих защите, будет различно.

Пример 4. При $k=3$ в треугольной системе хэш-кодов количество подблоков данных, подлежащих защите, будет равняться 6, в квадратной системе хэш-кодов — 9, в трехмерной (куб) — 48.

Для оценивания разработанных систем хэш-кодов рассмотрим несколько вариантов их построения (табл. 4),

Таблица 3

Характеристики разработанных систем хэш-кодов

№ п/п	Наименование системы хэш-кодов		Размер системы хэш-кодов	Характеристики системы хэш-кодов	
				Количество подблоков блока данных	Количество хэш-кодов
1.1	Системы в двумерном пространстве	Прямоугольные системы хэш-кодов	$\left((k+1)\cdot(t+1)-1\right)$	$k\cdot t$	$k+t$
1.2		Квадратные системы хэш-кодов	$\left((k+1)^2-1\right)$	k^2	$2k$
1.3		Треугольные системы хэш-кодов	$\left(\frac{k(k+1)}{2}+k+1\right)$	$\frac{k(k+1)}{2}$	$k+1$
2.	Системы в n-мерном пространстве (кубические системы хэш-кодов)		$(k+1)^3$	$k(k+1)^2$	$(k+1)^2$

Таблица 4

Объемы вводимой избыточности для вариантов построения разработанных систем хэш-кодов

№ п/п	Наименование систем хэш-кодов		Характеристики	Варианты построения разработанных систем								
				1 вариант	2 вариант	3 вариант	4 вариант	5 вариант	6 вариант	7 вариант	8 вариант	9 вариант
1.	Системы в двумерном пространстве	Прямоугольные системы хэш-кодов	Количество подблоков данных	6	12	20	54	120	144	176	216	280
			Количество хэш-кодов	5	7	9	15	22	25	27	30	34
			Объем избыточности	≈83%	≈58%	45%	≈28%	≈18%	≈17%	≈15%	≈14%	≈12%
2.		Квадратные системы хэш-кодов	Количество подблоков данных	9	16	25	64	121	144	196	225	289
			Количество хэш-кодов	6	8	10	16	22	24	28	30	34
			Объем избыточности	≈67%	50%	25%	25%	≈18%	≈17%	≈14%	≈13%	≈12%
3.		Треугольные системы хэш-кодов	Количество подблоков данных	6	21	55	120	171	210	231	253	276
			Количество хэш-кодов	4	7	11	16	19	21	22	23	24
			Объем избыточности	≈67%	≈33%	20%	≈13%	≈11%	10%	≈10%	≈9%	≈8%
4.	Системы в *n*-мерном пространстве (кубические системы хэш-кодов)		Количество подблоков данных	18	48	100	180	294	-	-	-	-
			Количество хэш-кодов	9	16	25	36	49	-	-	-	-
			Объем избыточности	50%	≈33%	25%	20%	≈17%	-	-	-	-

отличающиеся количеством подблоков данных, подлежащих защите, и вычислим соответствующие им объемы вводимой избыточности.

На рис. 14 представлен график со сравнительной оценкой разработанных систем хэш-кодов, из которого видно, что более выигрышными являются треугольные, затем квадратные, прямоугольные, а потом кубические системы хэш-кодов.

Однако, кубическим конструкциям присущи отличительные свойства, связанные с кратностью гарантировано обнаруживаемых и локализуемых подблоков данных в случае нарушения их целостности.

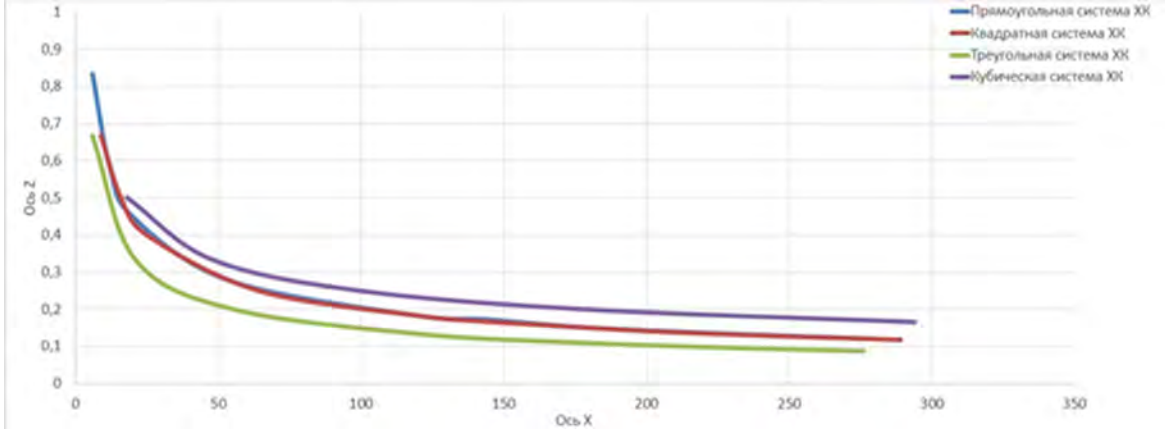

Рис. 14. График со сравнительной оценкой разработанных систем хэш-кодов

Заключение

Таким образом, представлен способ снижения вводимой при контроле целостности данных избыточности на основе разработанных по правилам построения помехоустойчивых кодов систем хэш-кодов. Результаты оценки показали, что разработанные конструкции позволяют сократить избыточность, связанную с вычислением контрольной информации, при заданном уровне защищенности данных.

Предложенный подход позволяет осуществить контроль целостности не только данных, подлежащих защите, но и самих эталонных хэш-кодов.

Литература

1. *Tchernykh A., Babenko M., Chervyakov N. and etc.* AC-RRNS: Anti-Collusion Secured Data Sharing Scheme for Cloud Storage // International Journal of Approximate Reasoning. Special Issue on Uncertainty in Cloud Computing: Concepts, Challenges and Current Solutions. 2018. Vol. 102. Pp. 60–73.

2. *Samoylenko D.V., Eremeev M.A., Finko O.A.* A method of providing the integrity of information in the group of robotic engineering complexes based on cryptcode constructions // Automatic Control and Computer Sciences. 2017. № 51:8. Pp. 965–971.

3. *Пойманова Е.Д., Татарникова Т.М.* Управление пространственными ресурсами систем хранения данных // Сборник трудов X международной научно-практической конференции «Программная инженерия и компьютерная техника (Майоровские чтения)». Санкт-Петербург, 2018. С. 85–88.

4. *Савин С.В., Финько О.А.* Обеспечение целостности данных в автоматизированных системах на основе линейных систем хэш-кодов // Научный журнал КубГАУ. № 114(10). 2015. URL: http://ej.kubagro.ru/2015/10/pdf/60.pdf (дата обращения 05.08.2020).

5. *Диченко С.А.* Контроль и обеспечение целостности информации в системах хранения данных // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 1. С. 49–57.

6. *Biham E., Dunkelman O.* A framework for iterative hash functions — HAIFA // Cryptology ePrint Archive. Report 2007/278. 2007. Pp. 1–20. URL: https://eprint.iacr.org/2007/278 (дата обращения 05.08.2020).

7. *Wang X., Yu H.* How to break MD5 and Other Hash Function // Advances in Cryptology — EUROCRYPT 2005. Lecture Notes in Computer Science. Springer-Verlag, 2005. Vol. 3494. Pp. 19–35.

8. *Bellare M.* New Proofs for NMAC and HMAC: Security without Collision-Resistance // Advances in Cryptology — CRYPTO 2006 Lecture Notes in Computer Science. Vol. 4117. Springer, Berlin, Heidelberg, 2006. Vol. 4117. Pp. 1–1.

9. *Финько О.А, Диченко С.А.* Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищённых информационно-аналитических систем // Вопросы кибербезопасности. 2019. № 6(34). С. 17–36.

10. *Finko O.A., Dichenko S.A.* Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions // Proceedings of the 2018 Multidisciplinary Symposium on Computer Science and ICT, Stavropol, Russia, October 15. 2018. 2254. CEUR Workshop Proceedings. 2018. Pp. 139–146.

11. *Диченко С.А.* Разработка алгоритма контроля и обеспечения целостности данных при их хранении в центрах обработки данных // Информационный бюллетень Омского научно-образовательного центра ОмГТУ и ИМ СО РАН в области математики и информатики Материалы VIII Международной молодежной научно-практической конференции с элементами научной школы. 2018. С. 110–113.

GENERALIZED METHOD OF APPLYING HASH FUNCTIONS FOR DATA INTEGRITY CONTROL

SERGEY A. DICHENKO

Krasnodar, Russia, dichenko.sa@yandex.ru

OLEG A. FINKO

Krasnodar, Russia, ofinko@yandex.ru,
www.mathnet.ru/eng/person40004

KEYWORDS: data storage system; data integrity control; cryptographic methods; hash function; reduction of introduced redundancy.

ABSTRACT

Data storage systems designed for storing large multidimensional arrays of information, functioning in conditions of destructive influences of an attacker and the environment, are considered. One of the most urgent tasks for such systems is the organization of secure data storage, and taking into account such operating conditions - ensuring their integrity. Ensuring data integrity is a difficult task, due to its complexity, as it includes both recovery and data integrity control. One of the well-known and widely used methods of data integrity control is the use of cryptographic methods, in particular, the hashing function. However, despite the widespread use of hash functions, they have been very little researched, and practical proposals for their use are very few and are characterized by a number

of disadvantages associated with the need to introduce a high redundancy of control information. In the context of limitations on the existing resource of data storage systems, this can lead to a decrease in the probability of completing the task of their functioning, or even to its failure. A generalized method is proposed, the use of which will reduce the amount of introduced redundancy when monitoring the integrity of information in data storage systems, based on the use of cryptographic hash functions, a distinctive feature of which is the use of rules for constructing error-resistant codes. In addition, the developed method provides the data integrity control procedure with a new property: the ability to control the integrity of not only the data to be protected, but also the reference hash codes themselves. Calculated data of the required volume of the introduced redundancy are obtained when monitoring the data integrity in existing storage systems using the developed method.

REFERENCES

1. Tchernykh A., Babenko M., Chervyakov N. and etc. AC-RRNS: Anti-Collusion Secured Data Sharing Scheme for Cloud Storage. *International Journal of Approximate Reasoning. Special Issue on Uncertainty in Cloud Computing: Concepts, Challenges and Current Solutions*. 2018. Vol. 102. Pp. 60–73.

2. Samoylenko D.V., Eremeev M.A., Finko O.A. A method of providing the integrity of information in the group of robotic engineering complexes based on cryptcode constructions. *Automatic Control and Computer Sciences*. 2017. № 51:8. Pp. 965–971.

3. Poimanova E.D., Tatarnikova T.M. Upravlenie prostranstvennymi resursami sistem hranenija danny [Management of spatial resources of data storage systems]. *Sbornik trudov X mezhdunarodnoj nauchno-prakticheskoj konferencii "Programmnaja inzhenerija i komp'juternaja tehnika (Majorovskie chtenija)"* [Proceedings of the X International Scientific and Practical Conference "Software Engineering and Computer Engineering (Major Readings)"]. St. Petersburg, 2018. Pp. 85–88. (In Rus)

4. Savin S.V., Finko O.A. Obespechenie celostnosti dannyh v avtomatizirovannyh sistemah na osnove linejnyh sistem hjesh-kodov [Ensuring data integrity in automated systems based on linear systems of hash codes]. *Nauchnyj zhurnal KubGAU* [Scientific journal KubGAU]. URL: http://ej.kubagro.ru/2015/10/pdf/60.pdf (date of access 10.12.2018). (In Rus)

5. Dichenko S.A. Control and security of information integrity in data storage systems. *H&ES Research*. 2019. Vol. 11. No 1. Pp. 49–57. (In Rus)

6. Biham E., Dunkelman O. A framework for iterative hash functions – HAIFA. *Cryptology ePrint Archive*. Report 2007/278. 2007. Pp. 1–20. URL: https://eprint.iacr.org/2007/278 (дата обращения 05.08.2020).

7. Wang X., Yu H. How to break MD5 and Other Hash Function. *Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science*. Springer-Verlag, 2005. Vol. 3494. Pp. 19–35.

8. Bellare M. New Proofs for NMAC and HMAC: Security without Collision-Resistance. *Advances in Cryptology – CRYPTO 2006 Lecture Notes in Computer Science*. Vol. 4117. Springer, Berlin, Heidelberg, 2006. Vol. 4117. Pp. 1–1.

9. Finko O.A., Dichenko S.A. Hybrid crypto-code method for monitoring and restoring data integrity for secure information and analytical systems. *Voprosy kiberbezopasnosti* [Cybersecurity Issues] 2019. No. 6(34). Pp. 17–36. (In Rus)

10. Finko O.A., Dichenko S.A. Two-dimensional control and assurance of data integrity in information systems based on residue number system codes and cryptographic hash functions. *Proceedings of the 2018 Multidisciplinary Symposium on Computer Science and ICT,* Stavropol, Russia, October 15. 2018. 2254. CEUR Workshop Proceedings. 2018. Pp. 139–146.

11. Dichenko S.A. Razrabotka algoritma kontrolja i obespechenija celostnosti dannyh pri ih hranenii v centrah obrabotki dannyh [Development of an algorithm for monitoring and ensuring the integrity of data during their storage in data processing centers]. *Informacionnyj bjulleten' Omskogo nauchno-obrazovatel'nogo centra OmGTU i IM SO RAN v oblasti matematiki i informatiki Materialy VIII Mezhdunarodnoj molodezhnoj nauchno-prakticheskoj konferencii s jelementami nauchnoj shkoly* [Newsletter of the Omsk Scientific and Educational Center of OmSTU and IM SB RAS in the field of mathematics and computer science Materials of the VIII International Youth Scientific and Practical Conference with elements of a scientific school]. 2018. Pp. 110–113. (In Rus)

INFORMATION ABOUT AUTHORS:

Dichenko S.A., PhD, Doctoral Candidate of the Krasnodar Higher Military School named after S.M.Shtemenko;

Finko O.A., PhD, Full Professor, Professor at the Department of the Krasnodar Higher Military School named after S.M.Shtemenko.

For citation: Dichenko S.A., Finko O.A. Generalized method of applying hash functions for data integrity control. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 48–59. doi: 10.36724/2409-5419-2020-12-6-48-59 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-60-67

МОДУЛЬ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ

ЕВГЛЕВСКАЯ
Наталья Валерьевна

АННОТАЦИЯ

На критически важном объекте система управления информационной безопасностью и система хакера, реализующего в отношении любых узлов информационно-коммуникационной сети этого объекта деструктивные компьютерные атаки, пребывают в состоянии противоборства. С одной стороны, хакер воздействует на объектовую информационно-коммуникационную сеть с целью осуществления основных этапов агентурной и технической компьютерной разведок с последующей реализацией деструктивных компьютерных атак. С другой стороны, система управления информационной безопасностью критически важного объекта обнаруживает несанкционированные действия хакера и реализует необходимые меры по их блокированию/нейтрализации/предотвращению. Как показывает практика, управляющие воздействия со стороны системы управления информационной безопасностью оказываются с задержкой, а чаще всего, когда хакер уже достиг поставленной цели. Для оперативности принятия решения по блокированию/нейтрализации/предотвращению деструктивных компьютерных атак со стороны хакера на узлы информационно-коммуникационной сети администратором по информационной безопасности критически важного объекта, предлагается применение модуля принятия решений системы управления информационной безопасностью информационно-коммуникационной сети. Особенностью данного модуля является возможность формирования перечня рациональных мероприятий по защите информационно-коммуникационной сети критически важного объекта с учетом особенностей построения сети, тактико-технических характеристик узлов сети, возможностей хакера. Основой модуля являются математические модели указанных выше процессов и методика выбора рациональных мероприятий по защите информационно-коммуникационной сети критически важного объекта. Методика позволяет установить возможные причины недостаточно высокой эффективности функционирования объектовой информационно-коммуникационной сети в условиях реализации хакером деструктивных компьютерных атак в отношении сетевых узлов.

Сведения об авторе:

к.т.н., преподаватель Военной академии связи имени маршала Советского Союза С.М.Буденного, г. Санкт-Петербург, Россия, n.evglevskaya@gmail.com

КЛЮЧЕВЫЕ СЛОВА: хакер; деструктивная компьютерная атака; информационно-коммуникационная сеть; угроза; информационная безопасность.

Для цитирования: *Евглевская Н.В.* Модуль принятия решений по управлению информационной безопасностью в информационно-коммуникационной сети // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 60–67. doi: 10.36724/2409-5419-2020-12-6-60-67

Введение

Внедрение в автоматизированные системы управления результатов основных сквозных цифровых технологий влечет за собой появление новых видов угроз безопасности информации, реализуя которые хакер осуществляет деструктивные компьютерные атаки (КА) на любые узлы информационно-коммуникационной сети (ИКС) критически важного объекта (КВО). В таких условиях общепринятые способы разработки системы обеспечения защиты информации, обрабатываемой ИКС, являются недостаточно эффективными. Это обусловлено тем, что, как правило, анализу подлежат частные угрозы информационной безопасности (ИБ) и реализуются типовые подходы по их блокированию/нейтрализации/предотвращению без учета архитектуры, места, роли, особенностей функционирования ИКС, участвующей в управлении технологическими и производственными процессами, реализуемыми на КВО [1].

Особенностью предлагаемого подхода к разработке модуля принятия решений (ПР) системы управления ИБ (СУИБ) ИКС КВО является его системность, позволяющая представить ИКС КВО как совокупность взаимоувязанных функциональных узлов ИКС и каналов связи, используя которые хакер способен осуществлять деструктивные КА на сеть связи. В структуру модуля включена система ПР, предоставляющая администратору по ИБ КВО перечень рациональных мероприятий, реализация которых способствует блокированию/нейтрализации/предотвращению актуальных угроз ИБ, деструктивных КА [1].

Общая структура модуля ПР СУИБ ИКС КВО

На рис. 1 представлена структура модуля ПР СУИБ ИКС КВО.

Важнейшей составляющей модуля ПР является подмодуль математического моделирования деструктивных КА и процесса добывания хакером данных по техническим каналам утечки информации (КУИ) на КВО (подмодуль 4). Данный подмодуль базируется на динамической модели противоборства СУИБ и системы хакера (СХ). Исходными данными для указанной динамической модели послужили результаты моделирования процессов реализации деструктивных КА хакера на ИКС КВО и функционирования ИКС КВО в условиях реализации деструктивных КА. Исходными данными для моделирования процесса реализации деструктивных (КА) хакера на ИКС КВО стали результаты моделирования следующих процессов: вскрытия хакером технических КУИ на КВО; установки закладочных устройств (ЗУ) в технические КУИ на КВО; внедрения компьютерных вирусов в узлы ИКС КВО; вскрытия ИКС КВО с использованием средств технической компьютерной разведки хакера. Для построения модели процесса вскрытия технических КУИ на КВО использованы результаты моделирования технических КУИ, выявленных на КВО. Процесс вскрытия ИКС КВО с помощью средств технической компьютерной разведки хакера разработан с помощью результатов, полученных при моделировании следующих процессов: определения технической роли узлов ИКС, идентифика-

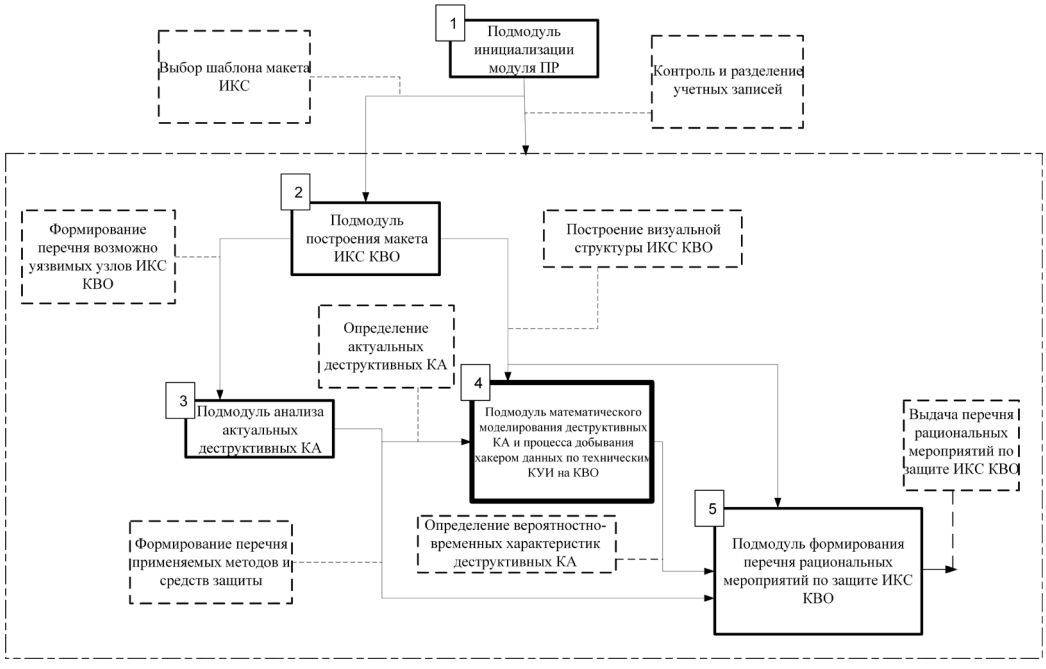

Рис. 1. Структура модуля ПР СУИБ ИКС КВО

ции узлов ИКС, операционной системы узлов ИКС и сервисов ИКС КВО. Для моделирования перечисленных процессов, а также процесса функционирования ИКС в условиях проведения хакером деструктивных КА используются базовые модели и методики оценки уровня ИБ, данные, характеризующие ИКС КВО.

С помощью данного подмодуля можно рассчитывать вероятностно-временные характеристики процессов реализации хакером деструктивных КА, а также создавать перечень тех КА, реализация которых возможна с наибольшей вероятностью. Также подмодуль 4 взаимодействует с системой мониторинга ИКС, обеспечивая при этом сбор статистических данных о деструктивных КА [1, 2].

В подмодуле анализа актуальных деструктивных КА (подмодуль 3) определяются актуальные деструктивные КА. Затем по результатам опроса пользователей/администратора по ИБ ИКС КВО, учитывая при этом применяемые способы защиты информации, выявляются узлы ИКС КВО, наиболее подверженные риску воздействия деструктивных КА, и актуальные деструктивные КА, которые хакер способен реализовать в отношении них. С целью облегчения процесса определения основных функциональных сетевых узлов, а также для того, чтобы сделать структуру ИКС КВО более наглядной, разработан подмодуль построения макета ИКС КВО (подмодуль 2). И, наконец, в подмодуле формирования перечня рациональных мероприятий по защите ИКС КВО (подмодуль 5) разрабатываются рекомендации администратору по ИБ для устранения уязвимостей системы защиты и предотвращения деструктивных КА. Контроль и разделение учетных записей на две категории: «Администратор» и «Пользователь» осуществляется в подмодуле инициализации модуля ПР (подмодуль 1). Учетная запись с категорией «Администратор» обеспечивает управление учетными записями и устанавливается для администратора по ИБ. Учетная запись с категорией «Пользователь» устанавливается для пользователей рабочих машин и блокирует возможность присвоения прав администратора неблагонадежным операторам [1–5].

Модели, входящие в состав подмодуля 4 [6–9], позволяют получить вероятностно-временные характеристики процессов реализации хакером деструктивных КА в отношении сетевых узлов КВО.

Методика выбора рациональных мероприятий по защите ИКС КВО

Для возможности адекватного выбора рациональных мероприятий по защите ИКС КВО, разработана методика, с использованием которой можно определить степень зависимости показателей оценки уровня ИБ ИКС КВО, соответствующих требованиям нормативных документов, а именно: $\overline{T}_{bezop.} \geq T_{treb.} = 24 chas.$, $P_{bezop.}(t) \geq P_{treb.} = 0{,}95$ [10], от значений и диапазонов возможного изменения частных параметров, используемых в качестве исходных данных. Изменению каждого частного параметра соответствует определенная совокупность рациональных организационно-технических мероприятий. Таким образом, определяя диапазон изменения частных параметров, можно выбрать такую совокупность рациональных организационно-технических мероприятий, реализация которой позволит ИКС КВО соответствовать требуемому уровню защищенности от деструктивных КА хакера.

Показателем степени зависимости обобщенного показателя защищенности ИКС КВО от деструктивных КА, реализуемых хакером, является приращение $\Delta P_{bezop.}(T_{treb.})$ значений вероятности пребывания ИКС КВО в безопасном состоянии за время $T_{treb.}$. При этом критерием выбора приращений является:m $\max\limits_{y} \left\{ \Delta P_{bezop.}\left(T_{treb.}, x_y\right), y = \overline{1, N} \right\}$, где x_y — частные показатели, используемые при моделировании в качестве исходных данных [6–9, 11].

Кроме используемых при моделировании частных показателей x_y, исходными данными являются и диапазоны их возможного изменения Δx_y, определяемые как разность их конечного x_{yk} и начального x_{yn} значений, т.е. $\Delta x_y = x_{yk} - x_{yn}$.

Постановка задачи

Дана монотонная функция $P_{bezop.}(t)$, характеризующая распределение времени пребывания ИКС КВО в безопасном состоянии. В общем случае, на указанное время и, следовательно, на характер изменения $\Delta P_{bezop.}(t)$ оказывает влияние ряд параметров $x_y, y = \overline{1, N}$, к*аждо*ый из которых может изменяться в определенных пределах между конечным x_{yk} и начальным x_{yn} значениями $\Delta x_y = x_{yk} - x_{yn}$.

Необходимо определить максимальные степени зависимости значений вероятности пребывания ИКС КВО в безопасном состоянии от значений и диапазонов изменения частных параметров с учетом вложенности моделей [6–9]: $N_y = \max f(\Delta P_{bezop.}(t)_{xy})$.

Решение

Для определения максимальных степеней N_y не требуется высокой точности расчета значений приращений целевой функции в зависимости от изменения ее аргументов, а необходим лишь знак этого приращения и номер соответствующего ему аргумента. Поэтому для простоты вычислений для решения поставленной задачи целесообразно воспользоваться градиентным методом Гаусса-Зейделя с учетом свойства вложенности моделей.

Чтобы определить значения $\Delta P_{bezop.}(t)_{xy}$, необходимо вычислить частные производные функции $P_{bezop.}(t, x_y)$ по каждому из параметров x_y, изменяющихся в некоторых пределах Δx_y. Это возможно, так как по условию $P_{bezop.}(t, x_y)$ является аналитической функцией в области опреде-

ления каждой переменной x_y, $y = \overline{1, N}$. Используя теорему Лагранжа, получается:

$$\Delta P_{wbezop.}\left(t, x_y, y = \overline{1, N}\right). \quad (1)$$

На рис. 2 представлен алгоритм выбора рациональных организационно-технических мероприятий по защите ИКС КВО.

На первом шаге алгоритма требуется ввести исходные данные [6–8]. На втором шаге производится расчет функции распределения $C(t)$ времени реализации деструктивных КА на ИКС КВО, $G(t)$ времени вскрытия ИКС КВО средствами технической компьютерной разведки, $F(t)$ времени вскрытия технических КУИ на КВО и внедрения в выявленные каналы ЗУ, вероятности $P_{bezop.}(t)$ пребывания ИКС КВО в безопасном состоянии. На третьем шаге необходимо сравнить вычисленное на втором этапе значение $P_{bezop.}(t)$ с требуемым значением [10]. Если критериальное условие выполняется, то подтверждается адекватность выполнения запланированных мероприятий по защите ИКС КВО, в противном случае требуется произвести расчет приращений $\Delta P_{bezop.}(T_{treb.})$ вероятности пребывания ИКС КВО в безопасном состоянии за время $T_{treb.}$. Затем производится расчет по формуле (1) $\{\Delta P_{bezop.}\}_w$. При этом j-му элементу

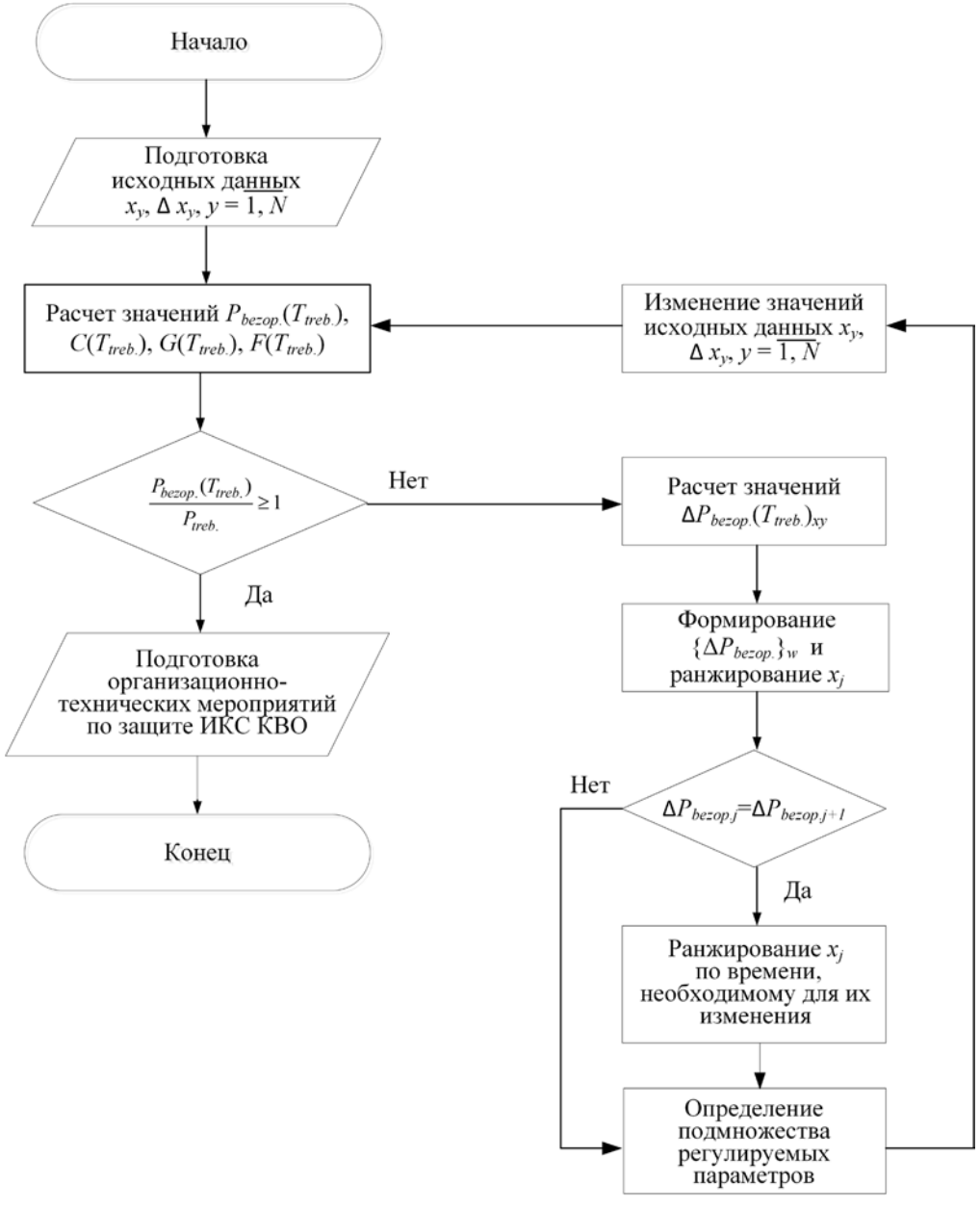

Рис. 2. Алгоритм выбора рациональных мероприятий по защите ИКС КВО

вектора $\{\Delta P_{bezop.}\}_w$ соответствует y-й параметр модели процесса функционирования ИКС КВО в условиях реализации хакером деструктивных КА [7]. Если вычисленное значение $P_{bezop.j}$ соответствует требуемому, производится ранжирование x_j. Если вычисленное значение $P_{bezop.j}$ ниже требуемого, необходимо определить регулируемые параметры и после изменения значений исходных данных произвести повторно расчет $C(T_{treb.})$, $G(T_{treb.})$, $F(T_{treb.})$, $P_{bezop.}(T_{treb.})$.

Пример расчета по методике

Для расчета используются исходные данные, характеризующие конфигурацию ИКС КВО, среду общего доступа, принципы, возможности, алгоритмы действий хакера [6–8, 10].

В связи с тем, что математические модели, входящие в подмодуль 4, обладают свойством вложенности, то поиск приращений $\Delta P_{bezop.}(T_{treb.})$ производится послойно.

На каждом слое модели противоборства СУИБ и СХ применяется формула (1) с тем лишь отличием, что на уровне выхода модели используется максимальное значение обобщенного показателя вероятности пребывания ИКС КВО в безопасном состоянии, а на уровне частных показателей используются минимальные значения, так как они характеризуют возможности хакера, реализующего деструктивные КА на узлы ИКС КВО.

В результате расчетов по формуле (1) получается семейство функций приращений обобщенного и частных показателей вероятности пребывания ИК $\Delta P_{ybezop.}\left(t, x_y, y=\overline{1,N}\right)$ С КВО в безопасном состоянии (рис. 3–6).

Чтобы обеспечить требуемый уровень защищенности сети связи, необходимо как сокращение времени восстановления ИКС, так и выполнение рациональных организационно-технических мероприятий, затрудняющих хакеру реализацию деструктивных КА на ИКС КВО.

Самыми существенными параметрами процесса реализации деструктивных КА на ИКС КВО являются следующие параметры: время вскрытия технических КУИ на КВО $t_{vskr.KUI}$ и время вскрытия ИКС КВО средствами технической компьютерной разведки хакера $t_{vskr.IKS}$ (рис. 3), длительность которых можно увеличить путем выполнения следующих организационно-технических мероприятий: расположение узлов ИКС КВО на максимально возможном удалении от границы контролируемой зоны (КЗ); проведение процедуры разграничения доступа персонала только к той аппаратуре, которая ему требуется для обеспечения технологического и производственного процессов; обеспечение экранирования кабелей и проводов; исключение из состава ИКС КВО незадействованной аппаратуры, неиспользуемых кабелей и проводов; применение систем маскирования ИКС КВО и ее параметров.

Наиболее существенными параметрами процесса вскрытия ИКС КВО средствами технической компьютерной разведки хакера являются: время идентификации узлов сети t_d и время сканирования портов и идентификации сетевых сервисов t_n (рис. 4), длительность которых можно увеличить путем выполнения таких организационно-технических мероприятий, как: проведение эмуляции виртуальных сетевых узлов, портов, сервисов; применение утилиты *Iptables*; использование метода «*Port knocking*».

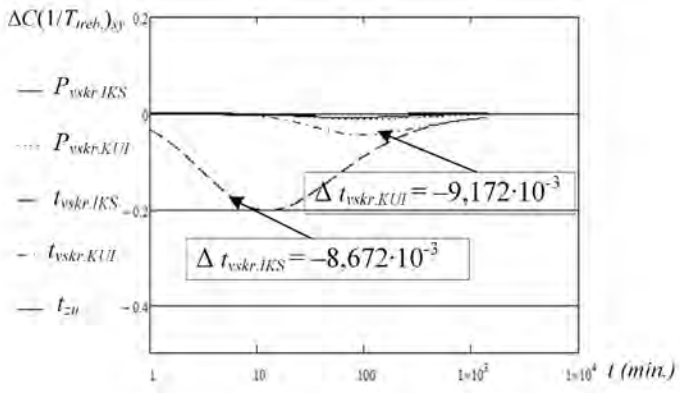

Рис. 3. Графики зависимостей $\Delta C(1/T_{treb.})_{xy}$

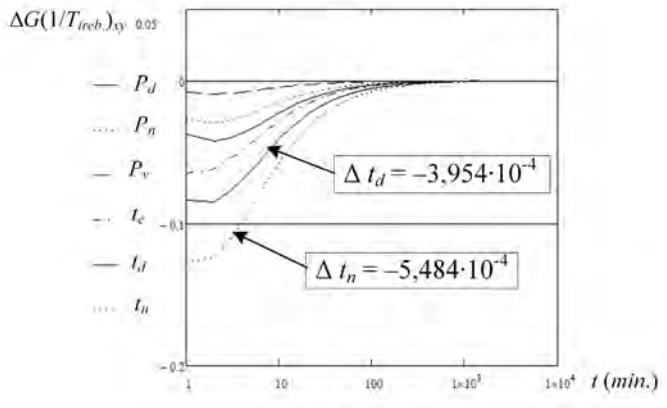

Рис. 4. Графики зависимостей $\Delta G(1/T_{treb.})_{xy}$

Наиболее существенными параметрами процесса вскрытия хакером технических КУИ на КВО являются: время вскрытия хакером акустического технического КУИ $t_{ak.}$, время внедрения ЗУ в технические КУИ t_{zu} (рис. 5). Затруднить хакеру реализовать данные действия могут такие организационно-технические мероприятия, как: обнаружение технических средств, использование которых не предусмотрено технологическим и производственным процессами; обнаружение неиспользуемых

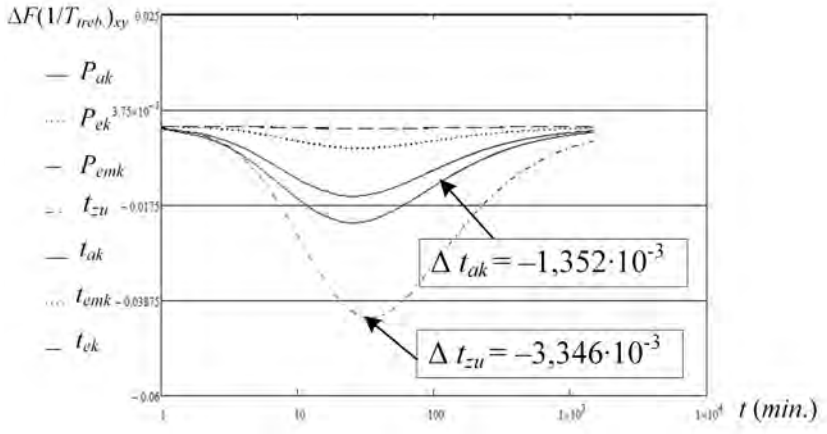

Рис. 5. Графики зависимостей $\Delta F(1/T_{treb.})_{xy}$

в технологическом и производственном процессах воздушных, подземных, наземных, проложенных в скрытой канализации кабельных линий, выходящих за пределы КЗ; использование метода противофазного подавления акустического сигнала; использование средств звукоизоляции и звукоглушения.

Анализ полученных результатов

На рис. 6 представлены графики, анализируя которые можно сделать вывод о том, что основным направлением для пребывания ИКС КВО в безопасном состоянии, согласно требованиям нормативных документов, является сокращение времени восстановления безопасного состояния ИКС КВО после успешной реализации хакером деструктивных КА.

На рис. 7 представлены вероятностно-временные характеристики пребывания ИКС КВО в безопасном состоянии при существующем порядке функционирования ИКС КВО и в случае применения модуля ПР СУИБ ИКС КВО, обеспечивающего уменьшение времени восстановления безопасного состояния ИКС КВО.

Заключение

Зависимости $P_{bezop.}(t)$, представленные на графиках рис. 7, позволяют оценить влияние времени восстановления безопасного состояния ИКС КВО $t_{vosst.}$ и времени реализации хакером деструктивных КА t_{ca} на продолжительность пребывания ИКС в безопасном состоянии. До применения модуля ПР и выполнения организационно-технических мероприятий, осложняющих хакеру реализацию деструктивных КА, время восстановления безопасного состояния ИКС КВО составляло $t_{vosst.}$ = 600 мин., длительность реализации хакером деструктивных КА составляло t_{ca} = 31 мин., при этом продолжительность пребывания сети в безопасном состоянии при $P_{treb.}$ = 0,95 составило 1,6 мин. (кривая 1). После применения модуля ПР и выполнения организационно-технических мероприятий

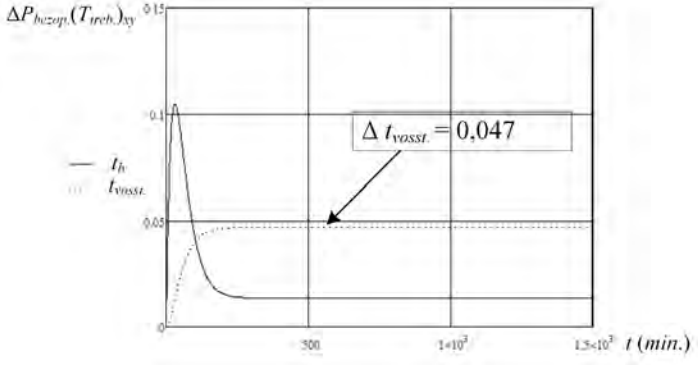

Рис. 6. Графики зависимостей $\Delta P_{bezop.}(T_{treb.})_{xy}$

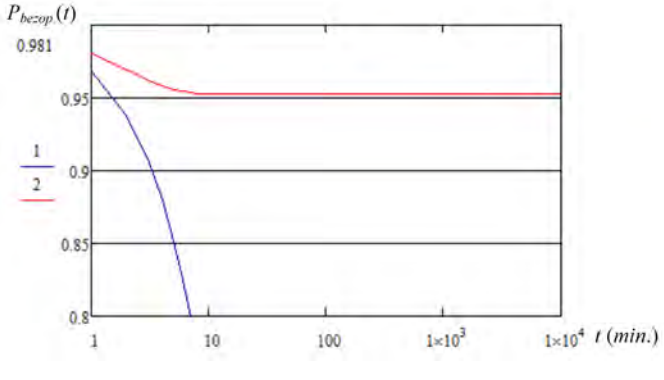

Рис. 7. Вероятностно-временные характеристики пребывания ИКС КВО в безопасном состоянии

время восстановления безопасного состояния ИКС КВО составило $t_{vosst.} = 2$ мин., $t_{ca} = 40$ мин., при этом вероятность пребывания ИКС в безопасном состоянии — не хуже 0,96 (кривая 2), что соответствует требованиям нормативных документов.

Разработанный модуль ПР СУИБ ИКС КВО позволяет администратору по ИБ оперативно принимать решения по управлению сетью, функционирующей в условиях реализации хакером деструктивных КА.

Литература

1. *Привалов А.А., Карабанов Ю.С., Королев А.И., Сидоров С.И.* Структура программного комплекса моделирования информационного конфликта системы безопасности телекоммуникационного объекта РЖД с подсистемой нарушителя // Интеллектуальные технологии на транспорте. 2015. № 1. С. 22–31.

2. *Королев А.И., Привалов А.А., Чимирзаев П.Э.* Модуль математического моделирования компьютерных атак и добывания нарушителем данных по техническим каналам утечки информации // Труды 70-й научно-технической конференции, посвященной Дню радио (Санкт-Петербург, 21–29 апреля 2015 г.). Санкт-Петербург, 2015. С. 314–315.

3. *Болтенкова Е.О., Кириленко В.О., Привалов А.А.* Модуль построения макета телекоммуникационного объекта ОАО «РЖД» // Труды 70-й научно-технической конференции, посвященной Дню радио (Санкт-Петербург, 21–29 апреля 2015 г.). Санкт-Петербург, 2015. С. 312–314.

4. *Карабанов Ю.С., Привалов А.А., Чимирзаев П.Э.* Модуль анализа потенциальных моделей угроз телекоммуникационных объектов ОАО «РЖД» // Труды 70-й научно-технической конференции, посвященной Дню радио (Санкт-Петербург, 21–29 апреля 2015 г.). Санкт-Петербург, 2015. С. 310–311.

5. *Карабанов Ю.С., Кириленко В.О, Привалов А.А.* Модуль инициализации программного комплекса анализа угроз безопасности телекоммуникационного объекта ОАО «РЖД» // Труды 70-й научно-технической конференции, посвященной Дню радио (Санкт-Петербург, 21–29 апреля 2015 г.). С.Петербург, 2015. С. 311–312.

6. *Евглевская Н.В., Привалов А.А., Скуднева Е.В.* Марковская модель конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя // Известия Петербургского университета путей сообщения. 2015. № 1 (42). С. 78–84.

7. *Evglevskaya N.V., Privalov A.A.* Information impact model at the telecommunication network objects // Scientific edition «Izvestiya of Petersburg State Transport University». 2015. No 1(42). Pp. 72–77.

8. *Привалов А.А., Евглевская Н.В, Привалов Ал.А.* Модель процесса вскрытия каналов утечки информации на объектах телекоммуникаций // Вопросы радиоэлектроники. 2014. № . 1. С. 156–161.

9. *Привалов А.А., Евглевская Н.В., Зубков К.Н.* Модель процесса вскрытия параметров сети передачи данных оператора *IP*-телефонной сети компьютерной разведкой организованного нарушителя // Научное издание «Известия Петербургского университета путей сообщения». 2014. № 2 (39). С. 106–111.

10. *Евглевская Н.В., Бекбаев Г.А., Привалов А.А., Шахматов Д.Н.* Модуль поддержки принятия решений по управлению информационной безопасностью телекоммуникационной сети единого дорожного диспетчерского центра управления перевозками ОАО «РЖД» на основе рационального выбора организационно-технических мероприятий // Известия Петербургского университета путей сообщения. 2016. № 2 (47). С. 161–171.

11. *Коцыняк М.А., Кулешов И.А., Лаута О.С.* Устойчивость информационно-телекоммуникационных сетей. СПб.: Санкт-Петербургский государственный политехнический университет, 2013. 92 с.

DECISION-MAKING MODULE FOR INFORMATION AND COMMUNICATIONS NETWORK INFORMATION SECURITY MANAGEMENT

NATALYA V.EVGLEVSKAYA

St. Petersburg, Russia, n.evglevskaya@gmail.com

KEYWORDS: hacker; deconstructive computer attack; information and communications network; threat; information security.

ABSTRACT

At a critical object information security management system and system of hacker, who realizes deconstructive computer attacks at any nodes of this object information and communications network are in confrontation. On the one hand, hacker influences at the object information and communications network for realizing main stages of agential and technical computer intelligences service and attacking afterwards. On the other hand, critical object information security management system finds unauthorized actions of hacker and realizes necessary measures to block/neutralize/prevent them. As practice shows, management impacts of information security management system make whith delay and most of all when hacker already has achieved the goal. For efficiency of decision-making for blocking/neutralization/prevention of deconstructive computer attacks from hacker at the information and communications network nodes by the information security administrator of critical object, decision-making module of information security management system of information

and communications network is offers. This module feature is the possibility of list formation of rational measures for protection critical object information and communications network considering network creation features, tactical and technical characteristics of network nodes, hacker opportunities. The module is based on mathematical models of the processes mentioned above and rational measures selection algorithm for protection of critical object information and communications network. Algorithm allows to find out possible reasons of insufficient efficiency of object information and communications network functioning in conditions when hacker realizes deconstructive computer attacks at network nodes.

REFERENCES

1. Privalov A.A., Karabanov Yu.S., Korolev A.I., Sidorov S.I. Software system structure of telecommunicational object safety system modelling with violator's subsystem. *Intellektual'nye tehnologii na transporte* [Intellectual technologies on transport]. 2015. No. 1. Pp. 22–31. (In Rus)
2. Korolev A.I., Privalov A.A., Chimirzaev P.E. Modul' matematicheskogo modelirovanija komp'juternyh atak i dobyvanija narushitelem dannyh po tehnicheskim kanalam utechki informacii [Mathematical simulation module of computer attacks and extraction by the data breacher through technical channels of information leakage]. *Trudy 70-j nauchno-tehnicheskoj konferencii, posvjashhennoj Dnju radio* [Proceedings of the 70-th scientific and technical conference dedicated to Radio Day, Saint Petersburg, on April 21–29, 2015]. Saint Petersburg, 2015. Pp. 314–315. (In Rus)
3. Boltenkova E.O., Kirilenko V.O., Privalov A.A. Modul' postroenija maketa telekommunikacionnogo ob'ekta OAO "RZhD" [Dummy creation module of JSCo "RZD" telecommunication object]. *Trudy 70-j nauchno-tehnicheskoj konferencii, posvjashhennoj Dnju radio* [Proceedings of the 70-th scientific and technical conference dedicated to Radio Day, Saint Petersburg, on April 21–29, 2015]. Saint Petersburg, 2015. Pp. 312–314. (In Rus)
4. Karabanov Yu.S., Privalov A.A., Chimirzaev P.E. Modul' analiza potencial'nyh modelej ugroz telekommunikacionnyh ob'ektov OAO "RZhD" [Module for analysis of threats potential models of JSCo "RZD" telecommunication objects]. *Trudy 70-j nauchno-tehnicheskoj konferencii, posvjashhennoj Dnju radio* [Proceedings of the 70-th scientific and technical conference dedicated to Radio Day, Saint Petersburg, on April 21–29, 2015]. Saint Petersburg, 2015. Pp. 310–311. (In Rus)
5. Karabanov Yu.S., Kirilenko V.O., Privalov A.A. Modul' inicializacii programmnogo kompleksa analiza ugroz bezopasnosti telekommunikacionnogo ob'ekta OAO "RZhD" [The program complex initialization module of the security threat analysis of JSCo "RZD" telecommunication object]. *Trudy 70-j nauchno-tehnicheskoj konferencii, posvjashhennoj Dnju radio* [Proceedings of the 70-th scientific and technical conference dedicated to Radio Day, Saint Petersburg, on April 21–29, 2015]. Saint Petersburg, 2015. Pp. 311–312. (In Rus)
6. Evglevskaya N.V., Privalov A.A., Skudneva E.V. Markov model of conflict of automated information processing and management systems with the system of destructive effects of an offender. *Izvestija Peterburgskogo universiteta putej soobshhenija* [Scientific edition «Izvestiya of Petersburg State Transport University»]. 2015. No. 1(42). Pp. 78–84. (In Rus)
7. Evglevskaya N.V., Privalov A.A. Information impact model at the telecommunication network objects. Izvestiya of Petersburg State Transport University. 2015. No. 1 (42). Pp. 72–77.
8. Privalov A.A., Evglevskaya N.V., Privalov Al.A. Model of the process for opening channels of information leakage on the objectes of the telecommunications. *Voprosy radiojelektroniki* [Radioelectronics questions]. 2014. No. 1. Pp. 156–161. (In Rus)
9. Privalov A.A., Evglevskaya N.V., Zubkov K.N. Model of the process for cracking the parameters pf data transmission network of IP-telephone system operator by the computer intelligence of organized intruder. *Izvestija Peterburgskogo universiteta putej soobshhenija* [Izvestiya of Petersburg State Transport University]. 2014. No. 2 (39). Pp. 106–111. (In Rus)
10. Evglevskaya N.V., Bekbaev G.A., Privalov A.A., Shakhmatov D.N. Decision-making support module for telecommunication network information security management of the joint road dispatching transportations management centre of russian railways JSCo based on rational choice of organisational and technical actions. *Izvestija Peterburgskogo universiteta putej soobshhenija* [Izvestiya of Petersburg State Transport University]. 2016. No. 2 (47). Pp. 161–171. (In Rus)
11. Kotsynyak M.A., Kuleshov I.A., Lauta O.S. *Ustojchivost' informacionno-telekommunikacionnyh setej* [Resistibility of information and telecommunications networks]. Saint Petersburg: Sankt-Peterburgskij gosudarstvennyj politehnicheskij universitet, 2013. 92 p. (In Rus)

INFORMATION ABOUT AUTHOR:

Evglevskaya N.V., PhD, lecturer at the Department of «Security of Special Purpose Information and Communications Systems» of Military Telecommunication Academy named after the Soviet Union Marshal Budienny S.M.

For citation: Evglevskaya N.V. Decision-making module for information and communications network information security management. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 60–67. doi: 10.36724/2409-5419-2020-12-6-60-67 (In Rus)

doi: 10.36724/2409-5419-2020-12-6-68-75

ФОРМАЛИЗАЦИЯ ИНФОРМАЦИОННОГО КОНФЛИКТА НА ОСНОВЕ ТЕОРИИ ДИНАМИЧЕСКИХ СИСТЕМ

МАМОНЧИКОВА
Алина Сергеевна

АННОТАЦИЯ

Постановка задачи: стремительное развитие средств дестабилизирующих воздействий на телекоммуникационную систему требует совершенствования научно-методического аппарата моделирования эффектов от таких воздействий. На сегодняшний день, недостаточно изученными остаются динамические процессы информационного конфликта в условиях совместного влияния средств дестабилизирующих воздействий и технических средств разведки на телекоммуникационную систему. **Проблемная ситуация:** наличие интегральных воздействий на телекоммуникационную систему технических средств разведки и средств дестабилизирующих воздействий, при отсутствии моделей, формализующих подобные трехсторонние взаимодействия. Направление формализации информационного конфликта на основе теории динамических систем с учетом временных параметров его развития разработано недостаточно глубоко. **Целью** является построение модели трехстороннего динамического информационного конфликта. **Используемые методы:** для построения математической модели информационного конфликта и ее исследования используется математический аппарат теории динамических систем. Сама модель представлена в виде системы дифференциальных уравнений. Предмет исследования: соотношение конкурентного распределения информационных ресурсов между сторонами информационного конфликта. **Объект исследования:** телекоммуникационная система в условиях влияния дестабилизирующих воздействий и технических средств разведки. **Научная новизна:** впервые для разрабатываемой модели представлены три стороны динамического конфликта, учитывающие развитие информационного конфликта во времени, рассматриваются различные степени конфликтного взаимодействия отдельных сторон, представлен синтез универсальных подходов, обобщающих динамический информационный конфликт трех сторон. **Практическая значимость:** предлагаемая модель может быть использована для исследования широкого класса конфликтных взаимодействий в прикладных областях в различных сферах. Найдет применение при рассмотрении подобных динамических конфликтов с участием трех и более сторон.

Сведения об авторе:

Соискатель ученой степени к.т.н., патентный поверенный РФ, специалист 1 кат. патентного бюро Публичного акционерного общества «Информационные телекоммуникационные технологии», г. Санкт-Петербург, Россия, alinitta33@mail.ru

КЛЮЧЕВЫЕ СЛОВА: динамический конфликт; динамические системы; формализация конфликта; информационный конфликт; многосторонний динамический конфликт.

Для цитирования: *Мамончикова А.С.* Формализация информационного конфликта на основе теории динамических систем // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 68–75. doi: 10.36724/2409-5419-2020-12-6-68-75

Введение

В настоящее время, ведется формирование методологии теории информационного противоборства в технической сфере. Одним из ключевых понятий информационного противоборства является информационный конфликт [1].

Для моделирования информационного конфликта может быть использован научно-методический аппарат (НМА), основанный на различных теориях, а, именно: теория марковских процессов; теория сетей Петри; теория стохастических сетей; теория игр; теория сложных иерархических систем и др. Однако, формализация информационного конфликта с помощью перечисленных НМА не учитывает представляющие интерес динамические характеристики процессов информационного конфликта.

К работам ученых специалистов, в которых рассматривается актуальное направление исследований информационного конфликта, основанное на научно-методическом аппарате теории динамических систем, можно отнести следующие работы: Н.Н. Толстых [2], А.Н. Асоскова [3], С.И. Макаренко [4, 5], Р.Л. Михайлова [6–9], В.И. Потапова [10], Г.А. Остапенко, Д.Г. Плотникова, Ю.Н. Гузева [11–14], Г.Е. Веселова, А.А. Колесникова [15], Е.Н. Надеждина [16], А.П. Петрова, А.И. Маслова, и др. [17], И.И. Семеновой, А.О. Мишурина [18], В.А. Шведовского, М.А. Петровой [19, 20]. Кроме того, подобные исследования ведутся и за рубежом (примером может являться работа [21]). В некоторых из этих работ, например [4], автор опирается на уже известные модели теории популяционной динамики, в которых задача моделирования конкурентной борьбы между различными биологическими видами является классической и хорошо исследованной. Известны работы различных ученых специалистов, которые описываются системой двух обыкновенных дифференциальных уравнений, например, модель Ланкастера[1]. Известна также работа А.К. Гришко, А.С. Жумабаевой, Н.К. Юркова [22], в которой описывается управление электромагнитной устойчивостью радиоэлектронных систем на основе вероятностного анализа динамики информационного конфликта. Отличительной особенностью вышеперечисленных работ является то, что в основу положены модели антогонистических двусторонних конфликтов, при этом модели трех и более сторон (многостороннего) информационного конфликта не рассматриваются. Таким образом, разработка модели трехстороннего динамического информационного конфликта является актуальной научной задачей.

1 Постановка задачи

Сформулируем частные научные задачи, решаемые в данной работе:

– разработка обобщенной модели трехстороннего динамического информационного конфликта;

– разработка частной модели трехстороннего динамического информационного конфликта.

Вначале, рассмотрим многосторонний динамический информационный конфликт сторон $i = 1,\ldots, n$. Введем допущение о том, что конфликт развивается на одном организационно-техническом уровне, и объектом конфликта служит некоторый глобальный информационный ресурс R, использующийся каждой стороной для своего функционирования[2]. Целью каждой i-ой стороны рассматриваемого динамического конфликта является максимизация эффективности своего функционирования, за счет максимизации доступного ей информационного ресурса $R_i \rightarrow \max$, как правило, за счет снижения ресурса противоборствующей стороны.

Для формализации задачи введем следующие обозначения:

A, B, C — стороны конфликтующих систем (для модели трехстороннего информационного конфликта);

t_0 — начальный момент времени конфликта;

t — время развития конфликта;

R — суммарный объем информационного ресурса;

R_i — информационный ресурс i-ой стороны;

$R_i(t_0)$ — значение ресурса i-ой стороны в начальный момент времени конфликта t_0;

α_i — коэффициент, определяющий возможности i-ой стороны по наращиванию количества ее ресурса R_i;

β_i — коэффициент, определяющий взаимную конкуренцию элементов i-ой стороны за ресурс R_i;

γ — коэффициент, определяющий снижение количества ресурса одной стороны, вследствие воздействия на него средств другой стороны.

При этом, информационный ресурс системы — количественная мера возможности выполнения задач по получению, передаче, обработке, хранению и представлению информации в интересах системы управления более высокого уровня.

При этом, в качестве примера, сторонами конфликта могут выступать: телекоммуникационная система (ТКС) — для стороны *A*; технические средства разведки (ТСР) — для стороны *B*, система дестабилизирующих воздействий (СДВ) — для стороны *C*.

[1] https://studme.org/169856/matematika_himiya_fizik/prostye_matematicheskie_modeli_realnyh_yavleniy (дата обращения 01.06.2020)

[2] Радзиевский В.Г., Сирота А.А. Информационное обеспечение радиоэлектронных систем в условиях конфликта. М.: ИПРЖР, 2001. 456 с.

2. Основная часть

2.1. Разработка обобщенной модели трехстороннего динамического информационного конфликта

В основу описания информационного конфликта положена известная модель Лотки-Вольтерры [23, 24]:

$$\frac{dR_i}{dt} = \alpha_i R_i - \beta_i R_i^2 - \sum_{\substack{i=1 \\ j=1 \\ i \neq j}}^{n} \gamma_{i,j} R_i R_j \qquad (1)$$

$$\sum_{\substack{i=1 \\ j=1 \\ i \neq j}}^{n} \gamma_{i,j} R_i R_j = \pm\gamma_{i,j} R_i R_j \pm \gamma_{i,(j+1)} R_i R_{(j+1)} \pm \ldots \pm \gamma_{n,(n-1)} R_n R_{(n-1)}$$

Тогда, обобщенная модель многостороннего информационного конфликта будет представлена в виде системы дифференциальных уравнений:

$$\begin{cases} \dfrac{dR_1}{dt} = \alpha_1 R_1 - \beta_1 R_1^2 \mp \gamma_{1,2} R_1 R_2 \mp \gamma_{1,3} R_1 R_3 \mp \ldots \mp \gamma_{1,n} R_1 R_n, \\ \ldots \\ \dfrac{dR_n}{dt} = \alpha_n R_n - \beta_n R_n^2 \mp \gamma_{n,(n-1)} R_n R_{(n-1)}. \end{cases} \qquad (2)$$

Остановимся на обобщенной модели трехстороннего конфликта, где стороны конфликтующих систем уже имеют буквенные обозначения *A, B, C*, которая будет выглядеть следующим образом:

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A^2 \mp \gamma_{AB} R_A R_B \mp \gamma_{AC} R_A R_C, \\ \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B^2 \mp \gamma_{BA} R_B R_A \mp \gamma_{BC} R_B R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C^2 \mp \gamma_{CA} R_C R_A \mp \gamma_{CB} R_C R_B. \end{cases} \qquad (3)$$

Следует отметить, что при рассмотрении сторон конфликта в количестве более трех, система будет иметь аналогичный вид системы дифференциальных уравнений, но с бо́льшим количеством уравнений, равным количеству рассматриваемых сторон.

Таким образом, разработана обобщенная модель трехстороннего динамического информационного конфликта, на основе которой будет решаться задача по формированию частной модели трехстороннего динамического информационного конфликта.

2.2. Разработка частной модели трехстороннего динамического информационного конфликта

Рассмотрим различные комбинации взаимодействия сторон, разложив полученную ранее систему (3) на множество систем, с учетом различных возможных вариантов взаимодействия сторон, выраженных различными знаками и значениями параметра γ в уравнениях (1–3).

Получаем следующие системы:

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A^2 - \gamma_{AB} R_A R_B - \gamma_{AC} R_A R_C, \\ \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B^2 - \gamma_{BA} R_B R_A - \gamma_{BC} R_B R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C^2 + \gamma_{CA} R_C R_A + \gamma_{CB} R_C R_B, \end{cases} \qquad (4)$$

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A^2 - \gamma_{AB} R_A R_B - \gamma_{AC} R_A R_C, \\ \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B^2 + \gamma_{BA} R_B R_A - \gamma_{BC} R_B R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C^2 + \gamma_{CA} R_C R_A + \gamma_{CB} R_C R_B, \end{cases} \qquad (5)$$

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A^2 - \gamma_{AB} R_A R_B - \gamma_{AC} R_A R_C, \\ \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B^2 + \gamma_{BA} R_B R_A + \gamma_{BC} R_B R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C^2 + \gamma_{CA} R_C R_A + \gamma_{CB} R_C R_B, \end{cases} \qquad (6)$$

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A^2 + \gamma_{AB} R_A R_B + \gamma_{AC} R_A R_C, \\ \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B^2 - \gamma_{BA} R_B R_A + \gamma_{BC} R_B R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C^2 - \gamma_{CA} R_C R_A - \gamma_{CB} R_C R_B, \end{cases} \qquad (7)$$

… и т. д.

При этом, «+», стоящий перед коэффициентом γ, указывает на взаимодействие сторон *A* и *B* (*A* и *C*, *B* и *C),* соответственно, при котором повышаются возможности по наращиванию информационных ресурсов, используемых

сторонами *A*, *B* или *C*; а «–», стоящий перед коэффициентом γ, указывает на взаимодействие сторон *A* и *B* (*A* и *C*, *B* и *C),* при котором снижаются возможности одной стороны по наращиванию используемого информационного ресурса, вследствие конкуренции других сторон между собой.

Ниже, для наглядности, на рис. 1 представлена схема частной модели трехстороннего информационного конфликта, с учетом одной выбранной комбинации взаимодействия сторон, представленной в системе (7), в качестве примера.

Остановимся на варианте модели, представленной в системе (7).

Далее, в основе лежит подход к исследованию рассматриваемой модели информационного конфликта, представленной системой (7), через редукцию, как операцию снижения размерности модели с трехмерной до двумерной. Получим проекции на различные плоскости: проекция на плоскость $R_A R_B$, при которой $R_C = 0$; проекция на плоскость $R_A R_C$, при которой $R_B = 0$; проекция на плоскость $R_B R_C$, при которой $R_A = 0$. Предлагаемый переход от трехмерного пространства к двумерному описан в работе[3].

При этом, получаем следующие системы (отдельно для каждой проекции):

– проекция на плоскость $R_A R_B$, при которой $R_C = 0$ (информационный ресурс стороны С):

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A{}^2 + \gamma_{AB} R_A R_B, \\ \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B{}^2 - \gamma_{BA} R_B R_A \end{cases} \quad (8)$$

– проекция на плоскость $R_B R_C$, при которой $R_A = 0$ (информационный ресурс стороны А):

$$\begin{cases} \dfrac{dR_B}{dt} = \alpha_B R_B - \beta_B R_B{}^2 + \gamma_{BC} R_B R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C{}^2 - \gamma_{CB} R_C R_B, \end{cases} \quad (9)$$

– проекция на плоскость$R_A R_C$, при которой $R_B = 0$ (информационный ресурс стороны В):

$$\begin{cases} \dfrac{dR_A}{dt} = \alpha_A R_A - \beta_A R_A{}^2 + \gamma_{AC} R_A R_C, \\ \dfrac{dR_C}{dt} = \alpha_C R_C - \beta_C R_C{}^2 - \gamma_{CA} R_C R_A. \end{cases} \quad (10)$$

Затем находим стационарное состояние систем, для получения стационарных решений уравнений систем, которые описывают распределение информационного ресурса в конфликте сторон, с учетом происходящих процессов.

Рассмотрим в качестве примера систему (9) с проекцией на плоскость $R_B R_C$. Найдем особые точки, в которых система находится в стационарном состоянии, приравняв производные dR_i/dt к нулю. Получаем:

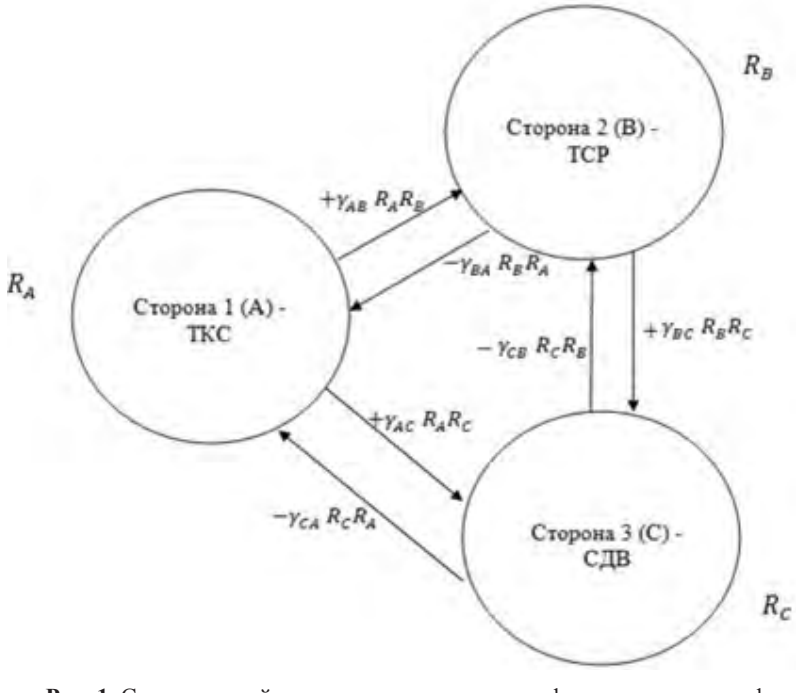

Рис. 1. Схема частной модели трехстороннего информационного конфликта

[3]Конкурентная динамика живых систем: Учебно-методическое пособие. Н. Новгород: НГУ им. Н.И. Лобачевского, 2010. 35 с.

$$\begin{cases} \alpha_B R_B - \beta_B R_B{}^2 + \gamma_{BC} R_B R_C = 0, \\ \alpha_C R_C - \beta_C R_C{}^2 - \gamma_{CB} R_C R_B = 0; \end{cases} \quad (11)$$

$$\begin{cases} R_B(\alpha_B - \beta_B R_B + \gamma_{BC} R_C) = 0, \\ R_C(\alpha_C - \beta_C R_C - \gamma_{CB} R_B) = 0; \end{cases} \quad (12)$$

Решая систему (12), находим стационарные точки:

A (0; 0; 0); B (0; α_B/β_B; 0); C (0; 0; α_C/β_C);

D (0, $\frac{\alpha_C\gamma_{BC} + \beta_C\alpha_B}{\gamma_{BC}\gamma_{CB} + \beta_B\beta_C}$, $\frac{-\alpha_B\gamma_{CB} + \beta_B\alpha_C}{\gamma_{CB}\gamma_{BC} + \beta_B\beta_C}$).

Найденные по аналогии стационарные точки для системы (10) выглядят следующим образом:

E (0; 0; 0); F (α_A/β_A; 0; 0); G (0; 0; α_C/β_C);

H ($\frac{\alpha_C\gamma_{AC} + \beta_C\alpha_A}{\gamma_{AC}\gamma_{CA} + \beta_A\beta_C}$; 0; $\frac{-\alpha_A\gamma_{CA} + \beta_A\alpha_C}{\gamma_{CA}\gamma_{AC} + \beta_A\beta_C}$);

Тогда, фазовые плоскости, построенные по найденным стационарным точкам будут выглядеть следующим образом (рис. 2):

Таким образом, решена задача по разработке частной модели трехстороннего динамического информационного конфликта.

Заключение

Как показало проведенное исследование, на основе теории динамических систем возможно построение моделей информационного конфликта, учитывающих сложный характер взаимодействия между сторонами.

При представлении информационного конфликта динамической моделью становится возможным детально исследовать развитие конфликта во времени, в зависимости от начального соотношения потенциалов сторон и параметров ТКС. Динамическая модель также позволяет выявить наиболее «сильные параметры» сторон, которые определяют траекторию развития конфликта, но данный вопрос является предметом дальнейших исследований по разработке методики достижения выигрыша ТКС в трехстороннем динамическом информационном конфликте.

К перспективным направлениям развития представленных моделей можно отнести исследование динамических конфликтов с более сложными вариантами конфликтного взаимодействия сторон и более глубоким изучением влияния сценариев поведения сторон на развитие и итог информационного конфликта.

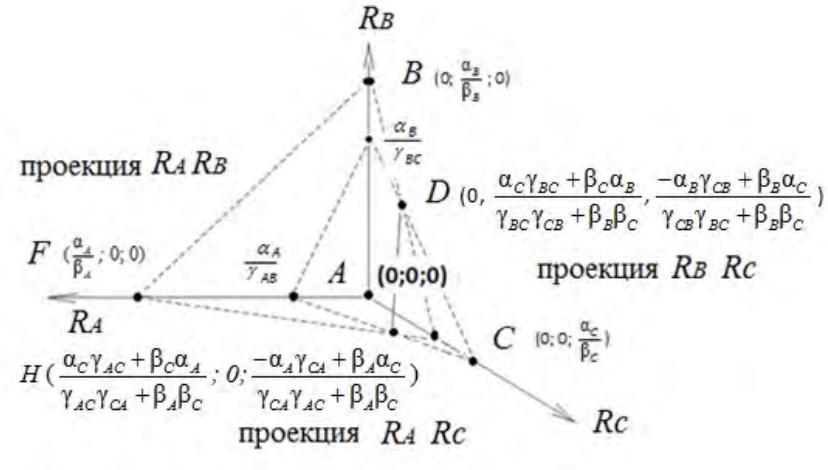

Рис. 2. Фазовые плоскости (вариант 1)

Литература

1. *Макаренко С. И.* Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122–185.

2. *Алферов А. Г., Власов Ю. Б., Толстых И. О., Толстых Н. Н., Челядинов Ю. В.* Формализованное представление эволюционирующего информационного конфликта в телекоммуникационной системе // Радиотехника. 2012. № 8. С. 27–33.

3. *Асосков А. Н., Малышева И. Н.* К вопросу о синтезе алгоритма управления инфокоммуникационной системы в условиях информационного конфликта // Теория и техника радиосвязи. 2011. № 4. С. 19–26.

4. *Макаренко С. И.* Модели воздействия средств радиоэлектронной борьбы на систему связи на основе методов популяционной динамики // Вестник Воронежского государственного технического университета. 2011. Т. 7. № 1. С. 96–99.

5. *Макаренко С. И.* Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса // Системы управления, связи и безопасности. 2017. № 1. С. 60–97.

6. Михайлов Р. Л. Модель динамической координации подсистем наблюдения и воздействия в информационном конфликте в виде иерархической дифференциальной игры трех лиц // Наукоемкие технологии. 2018. Т. 19. № 10. С. 44–51.

7. *Михайлов Р. Л., Ларичев А. В., Смыслова А. Л., Леонов П. Г.* Модель распределения ресурсов в информационном конфликте организационно-технических систем // Вестник Череповецкого государственного университета. 2016. № 6 (75). С. 24–29.

8. *Михайлов Р. Л., Поляков С. Л.* Модель оптимального распределения ресурсов и исследование стратегий действий сторон в ходе информационного конфликта // Системы управления, связи и безопасности. 2018. № 4. С. 323–344.

9. Михайлов Р. Л., Шишков А. И. Принципы координации подсистем наблюдения и воздействия // Научная мысль. 2017. Т. 1. № 3 (25). С. 38–43.

10. *Потапов В. И.* Математические модели динамических технических объектов конфликтных ситуаций — Омск: 2017.

11. *Остапенко Г. А., Плотников Д. Г., Гузев Ю. Н.* Особенности конфликтологии взвешенных сетей: понятие сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 1. С. 136–137.

12. *Остапенко Г. А., Плотников Д. Г., Гузев Ю. Н.* Формализация описания сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 2. С. 232–237.

13. *Остапенко Г. А., Плотников Д. Г., Гузев Ю. Н.* Стратегии сетевого противоборства // Информация и безопасность. 2016. Т. 19. № 2. С. 250–253.

14. *Остапенко Г. А., Плотников Д. Г., Гузев Ю. Н.* Динамика развития сетевого конфликта // Информация и безопасность. 2016. Т. 19. № 2. С. 278–279.

15. *Веселов Г. Е., Колесников А. А.* Синергетический подход к обеспечению комплексной безопасности сложных систем // Известия ЮФУ. Технические науки. 2012. № 4 (129). С. 8–18.

16. Надеждин Е. Н. Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства // Научный вестник. 2015.·№ 2 (4). С. 49–58.

17. *Петров А. П., Маслов А. И., Цаплин Н. А.* Моделирование выбора позиций индивидами при информационном противоборстве в социуме // Математическое моделирование. 2015. Т. 27. № 12. С. 137–148.

18. *Семенова И. И., Мишурин А. О.* Система управления моделями в области информационного противоборства // Вестник Саратовского государственного технического университета. 2010. Т. 4. № 1 (49). С. 150–160.

19. *Шведовский В. А., Петрова М. А.* Математическое моделирование напряженности этно-политического конфликта // Социология: методология, методы, математическое моделирование. 2001. № 14. С. 151–175.

20. *Шведовский В. А.* Динамическая модель электорального поведения // Математическое моделирование. 2000. Т. 12. № 8. С. 46–56.

21. U*dwadia F., Leitmann G. E., Lambertini L.* A Dynamical model of terrorism. Discrete Dynamics in Nature and Society. 2006. Vol. 2006. Article ID85653. Pp. 1–32. doi: 10.1155/DDNS/2006/85653.

22. *Гришко А. К., Жумабаева А. С., Юрков Н. К.* Управление электромагнитной устойчивостью радиоэлектронных систем на основе вероятностного анализа динамики информационного конфликта // Измерение. Мониторинг. Управление. Контроль. 2016. № 4 (18). С. 66–75.

23. *Макаренко С. И.* Моделирование совместного использования ресурсов системы связи методами популяционной динамики // Вестник Воронежского государственного технического университета. 2010. Т. 6. № 9. С. 63–65.

24. *Базыкин А. Д.* Нелинейная динамика взаимодействующих популяций. М.; Ижевск: Институт компьютерных исследований, 2003. 368 с.

FORMALIZATION OF INFORMATION CONFLICT BASED ON DYNAMIC SYSTEMS THEORY

ALINA S. MAMONCHIKOVA
St-Petersburg, Russia, alinitta33@mail.ru

KEYWORDS: dynamic conflict; dynamic systems; formalization of the conflict; information conflict; multilateral dynamic conflict.

ABSTRACT

Setting the task: the progressive development of means of destabilizing effects on the telecommunication system requires improvement of the scientific and methodological apparatus for modeling effects from such effects. To date, dynamic processes of information conflict remain insufficiently studied in conditions of joint influence of means of destabilizing effects and technical means of exploration on telecommunication system. Problem situation: presence of integral effects on telecommunication system of technical means of exploration and means of destabilizing effects, in the absence of models formalizing such tripartite interactions. The direction of formalization of information conflict on the basis of the theory of dynamic systems taking into account the time parameters of its development is not sufficiently developed. The goal is to build a model of a three-way dynamic information conflict. Methods used: mathematical apparatus of dynamic systems theory is used to construct a mathematical model of information conflict and its research. The model itself is represented as a system of differential equations. The subject of the study is the ratio of competitive distribution of information resources between the parties to the information conflict. Object of research: telecommunication system under the influence of destabilizing effects and technical means of exploration. Scientific novelty: for the first time for the developed model three sides of dynamic conflict are presented, taking into account the dynamics of development of information conflict in time, different degrees of conflict interaction between individual parties are taken into account, synthesis of universal approaches generalizing dynamic information conflict between the three sides is presented. Practical significance: The proposed model can be used to explore a broad class of conflict interactions in application areas in different spheres. It will be useful in dealing with such dynamic conflicts involving three or more parties.

REFERENCES

1. Makarenko S.I. Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression. *Systems of Control, Communication and Security*. 2015. No. 3. Pp. 122–185 (date of access 23.08. 2016). (In Rus)

2. Alferov A.G., Vlasov J.B., Tolstykh I.O., Tolstykh N.N., Chelajdinov J.V. The formalized representation of the evolving information conflict in telecommunication system. *Radiotekhnika*. 2012. No. 8. Pp. 27–33. (In Rus)

3. Asoskov A.N., Malysheva I.N. On infocommunication system management algorithm synthesis under information conflict conditions. Teoriia i tekhnika radiosviazi. 2011. No. 4. Pp. 19–26. (In Rus)

4. Makarenko S.I. Modeli vozdejstviya sredstv radioelektronnoj bor'by na sistemu svyazi na osnove metodov populyacionnoj dinamiki [Models of effects of electronic warfare means on communication system based on methods of population dynamics]. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Journal of the Voronezh State Technical University]. 2011. Vol. 7. No. 1. Pp. 96–99. (In Rus)

5. Makarenko S.I. Dinamicheskaya model' dvunapravlennogo informacionnogo konflikta s uchetom vozmozhnostej storon po nablyudeniyu, zahvatu i blokirovke resursa [Dynamic model of bidirectional information conflict taking into account the capabilities of the parties to monitor, seize and block the resource]. *Sistemy upravleniya, svyazi i bezopasnosti* [Control, communication and security systems]. 2017. No. 1. Pp. 60–97. (In Rus)

6. Mihajlov R.L. Model' dinamicheskoj koordinacii podsistem nablyudeniya i vozdejstviya v informacionnom konflikte v vide ierarhicheskoj differencial'noj igry trekh lic [Model of dynamic coordination of observation and impact subsystems in information conflict in the form of hierarchical differential game of three persons]. *Naukoemkie tekhnologii* [Knowledge-intensive technologies]. 2018. Vol. 19. No.10. Pp. 44–51. (In Rus)

7. Mihajlov R.L., Larichev A.V., Smyslova A.L., Leonov P.G. Model' raspredeleniya resursov v informacionnom konflikte organizacionno-tekhnicheskih system [Model of resource allocation in information conflict of organizational and technical systems]. *Vestnik Cherepoveckogo gosudarstvennogo universiteta* [Journal of Cherepovets State University]. 2016. No. 6 (75). Pp. 24–29. (In Rus)

8. Mihajlov R.L., Polyakov S.L. Model' optimal'nogo raspredeleniya resursov i issledovanie strategij dejstvij storon v hode informacionnogo konflikta [Model of optimal allocation of resources and study of strategies of actions of the parties during information conflict]. *Sistemy upravleniya, svyazi i bezopasnosti* [Management, communication and security systems]. 2018. No. 4. Pp. 323–344. (In Rus)

9. Mihajlov R.L., Shishkov A.I. Principy koordinacii podsistem nablyudeniya i vozdejstviya [Principles of Coordination of Observation and Impact Subsystems]. *Nauchnaya mysl'* [Scientific Thought]. 2017. Vol. 1. No. 3 (25). Pp. 38–43. (In Rus)

10. Potapov V.I. *Matematicheskie modeli dinamicheskih tekhnicheskih ob"ektov konfliktnyh situacij* [Mathematical models of dynamic technical objects of conflict situations]. Omsk, 2017. (In Rus)

11. Ostapenko G.A., Plotnikov D.G., Guzev Y.N. Features of conflictology of the weighed networks: concept of the network conflict. *Informatsiia i bezopasnost.* 2016. Vol. 19. No. 1. Pp. 136–137. (In Rus)
12. Ostapenko G.A., Plotnikov D.G., Guzev Y.N. Formalization of the description of the network conflict. *Informatsiia i bezopasnost*. 2016. Vol. 19. No. 2. Pp. 232–237. (In Rus)
13. Ostapenko G.A., Plotnikov D.G., Guzev Y.N. Strategy of network oppositon. *Informatsiia i bezopasnost*. 2016. Vol. 19. No. 2. Pp. 250–253. (In Rus)
14. Ostapenko G.A., Plotnikov D.G., Guzev Y.N. Dinamics of development of the network conflict. *Informatsiia i bezopasnost.* 2016. Vol. 19. No. 2. Pp. 278–279. (In Rus)
15. Veselov G.E., Kolesnikov A.A. Sinergeticheskii podkhod k obespecheniiu kompleksnoi bezopasnosti slozhnykh sistem [A synergistic approach to ensuring overall security of complex systems]. *Izvestiya SFedU. Engineering Sciences*. 2012. Vol. 129. No. 4. Pp. 8–18. (In Rus)
16. Nadezhdin E.N. Evaluation of the effectiveness of the protection mechanism of network resources based gaming model of information warfare. *Science Bulletin.* 2015.·Vol. 4. No. 2. Pp. 49–58. (In Rus)
17. Petrov A.P., Maslov A.I., Tsaplin N.A. Modeling of Making Choices by Individuals During Information Warfare in Society. *Mathematical Models and Computer Simulations.* 2015.·Vol. 27. No .12. Pp. 137–148 (In Rus)
18. Semenova I.I., Mishurin A.O. Management System Model of Information Counterforce. *Vestnik Saratov State Technical University.* 2010.·Vol. 4. No. 1. Pp. 150–160. (In Rus)
19. Shvedovskii V.A., Petrova M.A. Matematicheskoe modelirovanie napriazhennosti etno-politicheskogo konflikta [Mathematical modeling of the tension of ethno-political conflict]. *Sociology: methodology, methods, mathematical modeling*. 2001. No. 14. Pp. 151–175. (In Rus)
20. Shvedovskii V.A. Dinamicheskaia model' elektoral'nogo povedeniia [A dynamic model of electoral behavior]. *Mathematical Models and Computer Simulations.* 2000. Vol. 12. No. 8. Pp. 46–56. (In Rus)
21. Udwadia F., Leitmann G.E., Lambertini L. A Dynamical model of terrorism. *Discrete Dynamics in Nature and Society*. 2006. Vol. 2006. Article ID85653. Pp. 1–32. doi: 10.1155/DDNS/2006/85653.
22. Grishko A.K., Zhumabaeva A.S., Yurkov N.K. Upravlenie elektromagnitnoj ustojchivost'yu radioelektronnyh sistem na osnove veroyatnostnogo analiza dinamiki informacionnogo konflikta [Electromagnetic stability management of radio electronic systems based on probabilistic analysis of information conflict dynamics]. *Izmerenie. Monitoring. Upravlenie. Kontrol'* [Measurement. Monitoring. Management. Control]. 2016. No. 4 (18). Pp. 66–75. (In Rus)
23. Makarenko S.I. Modelirovanie sovmestnogo ispol'zovaniya resursov sistemy svyazi metodami populyacionnoj dinamiki [Modeling of joint use of communication system resources by methods of population dynamics]. *Journal of the Voronezh State Technical University.* 2010. Vol. 6. No. 9. Pp. 63–65. (In Rus)
24. Bazykin A.D. *Nelinejnaya dinamika vzaimodejstvuyushchih popu-lyacij* [Nonlinear dynamics of interacting populations]. Moscow, Izhevsk: Institute of Computer Research, 2003. 368 p. (In Rus)

INFORMATION ABOUT AUTHOR:
Mamonchikova A.S., applicant of an academic degree, Russian patent attorney 1 category specialist of the Patent Office of PJSC "Inteltech".

For citation: Mamonchikova A.S. Formalization of information conflict based on dynamic systems theory. *H&ES Research*. 2020. Vol. 12. No. 6. Pp. 68–75. doi: 10.36724/2409-5419-2020-12-6-68-75 (In Rus)

ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

Редакция журнала H&ES Research принимает к публикации статьи на русском и английском языках. Предоставляемая рукопись должна быть актуальной, обладать новизной, отражать постановку задачи, содержать описание основных результатов исследования, выводы, а также соответствовать указанным ниже правилам оформления. Текст должен быть тщательно вычитан автором, который несет ответственность за научнотеоретический уровень публикуемого материала.

Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, аннотация, ключевые слова, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями рисунков в формате TIFF, EPS по требованиям указанным в п.7.

К статье прилагается экспертное заключение о возможности опубликования статьи в открытой печати и две рецензии кандидатов или докторов наук по профилю планируемой публикации материалов (сканированные копии в электронном виде).

Все материалы высылаются электронной почтой в адрес журнала: HT-ESResearch@yandex.ru.

1. **Статья подготавливается** в редакторе MS Word. Шаблон статьи можно скачать на сайте журнала www.h-es.ru.

2. **Данные об авторе:** фамилия, имя, отчество, ученая степень, звание, должность и полное название организации – места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.

3. **Объем аннотации** 200–250 слов. Аннотация должна быть информативной (не содержать общих слов), без сокращений, структурированной, отражать основное содержание статьи: предмет, цель, методологию проведения исследований, результаты исследований, область их применения, выводы. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье. Предложения должны начинаться словами: показано, получено, исследовано, предсказано и т.д. и т.п.

4. **Ключевые слова:** от 5 до 7 слов (словосочетаний), разделенных точкой с запятой.

5. **Объём статьи** без аннотации – от 15 до 30 тыс. знаков с пробелами. Рисунки и таблицы в объеме статьи не учитываются.

6. **Формульные выражения** выполняются в редакторе Math Type. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается. Длина формулы в одну строчку 8–9 см.

Простые формулы и буквенные обозначения величин следует писать в строку обычным текстом. В формулах использовать только буквы латинского и греческого алфавита!

Размеры шрифтов (Size) предварительно перед набором первой формулы установить (в MathType) следующие: кегль основной – 10, крупный индекс – 7, мелкий индекс – 5, крупный символ – 12, мелкий символ – 8. Формулы, не содержащие специальных математических символов, должны быть набраны в тексте (в формате Word). Греческие обозначения, скобки (квадратные и круглые) и цифры всегда набираются прямым шрифтом. Латинские буквы набираются курсивом как в формулах, так и в тексте, кроме устойчивых форм (max, min, cos, sin, tg, log, exp, det …).

Нельзя использовать сканированные формулы! Все формулы должны быть набраны вручную!

7. **Рисунки и таблицы** в статье должны быть пронумерованы и снабжены подписями, в тексте статьи должны иметься ссылки на каждый рисунок и таблицу (рис.1 и табл.1). Если рисунок или таблица единственные в статье, то их не нумеруют.

Рисунки должны быть четкими, с хорошо проработанными деталями. Избегать текстовых надписей на иллюстрациях. Заменять их цифровыми обозначениями, которые поясняются в подписи или в основном тексте. Все рисунки прилагаются в виде отдельных файлов в формате TIFF, EPS с разрешением не менее 300 dpi для оригинального размера в печатном издании (для больших рисунков ширина от 14 до 20 см, для маленьких от 7 до 9 см).

8. **Список литературы:** от 15 до 50 наименований. Из них самоцитирований не должно быть более 25%. В числе источников желательно не менее 50 % иностранных источников (для статей на английском языке – 15% российских). Состав источников должен быть актуальным и содержать не менее 8 статей из научных журналов не старше 10 лет, из них 4 – не старше 3 лет.

Ссылки должны быть только на статьи, патенты, книги и статьи из сборников трудов. В списках литературы не размещать ГОСТЫ, рекомендации, диссертации, авторефераты и другую нормативную и непериодическую документацию. Эти данные можно указывать в теле статьи в скобках или в виде постраничных сносок (если автор непременно хочет указать нормативный документ или сослаться на свою диссертацию). Список литературы оформляется в соответствии с ГОСТ 7.052008. **Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.**

9. **На английском языке** предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Все названия издательств и журналов должны быть транслитерированы, а не переведены. Названия организаций в списках литературы (Труды Академии...) должны быть четко выверены с данными организации и иметь официальное английское наименование, которое указано на их сайте или также транслитерированы. Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.

10. **Структура статьи на английском языке**

Introduction (введение)

Materials and methods (материалы и методы).

Results and Discussions (результаты и обсуждение).

Conclusions (вывод)

Acknowledgements (благодарности, необязательный раздел)

References (ссылки на использованную литературу)

На руском языке предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Внимание! Редакция оставляет за собой право отклонить представленные материалы, оформленные не по указанным правилам.