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)

ПЛАТА С АСПИРАНТОВ ЗА ПУБЛИКАЦИЮ РУКОПИСИ НЕ ВЗИМАЕТСЯ

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.**
Все номера журнала находятся в свободном доступе на сайте.

Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.

POSTGRADUATE STUDENTS FOR PUBLICATION OF THE MANUSCRIPT WILL NOT BE CHARGED

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.**
All issues of the journal are in a free access on a site.

Language of publications: Russian, English.
Periodicity – 6 issues per year.

5 2019

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU

Учредитель:
ООО «ИД Медиа Паблишер»

Издатель:
СВЕТЛАНА ДЫМКОВА

Главный редактор:
КОНСТАНТИН ЛЕГКОВ

H&ES Research зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.
Издательская лицензия
ПИ № ФС 77-60899.

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.

Дизайн и компьютерная верстка:
ОКСАНА ИВАНОВА

СОДЕРЖАНИЕ

РАДИОТЕХНИКА И СВЯЗЬ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ПУБЛИКАЦИИ НА АНГЛИЙСКОМ ЯЗЫКЕ
РАДИОТЕХНИКА И СВЯЗЬ

CONTENTS

Founder:
"Media Publisher", LLC

Publisher:
SVETLANA DYMKOVA

Journal H&ES Research has been registered by the Federal service on supervision of legislation observance in sphere of mass communications and cultural heritage protection.
Publishing license
ПИ № ФС 77-60899.

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.

Design and computer imposition:
OKSANA IVANOVA

doi: 10.24411/2409-5419-2018-10282

АДАПТИВНЫЙ МЕТОД ОБНАРУЖЕНИЯ АНОМАЛИЙ ТРАФИКА В ВЫСОКОСКОРОСТНЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

АГЕЕВ
Сергей Александрович[1]

ГЛАДКИХ
Анатолий Афанасьевич[2]

КУРНОСОВ
Валерий Игорьевич[3]

ПРИВАЛОВ
Андрей Андреевич[4]

АННОТАЦИЯ

В работе предложен и исследован адаптивный эвристический (поведенческий) метод обнаружения аномалий трафика в высокоскоростных мультисервисных сетях связи, функционирующий в режиме реального времени. Актуальность данного исследования обусловлена тем, что многие процессы управления информационной и сетевой безопасностью, а также процессы управления рисками реализаций их угроз в высокоскоростных мультисервисных сетях связи необходимо реализовывать в режиме близком к режиму реального времени. В основу предлагаемого в работе подхода положена концепция условной нелинейной Парето – оптимальной фильтрации В. С. Пугачева. Суть данного подхода заключается в том, что оценка параметра трафика производится в два этапа: на первом этапе производится оценка прогноза значений параметров, а на втором, с получением следующих наблюдений параметров, корректировка их значений. В предлагаемых методе и алгоритме прогнозы значений параметров трафика производятся в небольшом по размеру скользящем окне, а адаптация реализуется на основе псевдоградиентных процедур, параметры которых регулируются с помощью метода нечеткого логического вывода Такаги – Сугено. Особенностью разработанных процедур оценки характеристик высокоскоростного трафика мультисервисных сетей связи является то, что они позволяют учитывать динамику изменения параметров сетевого трафика. Предложенный метод и алгоритм относятся к классу адаптивных методов и алгоритмов с предварительным обучением. Средняя относительная погрешность оценки оцениваемых параметров трафика не превышает 10 %, что является достаточным значением для реализации задач оперативного сетевого управления. Процедура обнаружения аномального поведения трафика высокоскоростной мультисервисной сети связи в работе реализована на основе метода нечеткого логического вывода Мамдани, в котором интервалы состояния параметров трафика определяются на основе принятой в сети политики безопасности. Проведенное в работе исследование предложенного метода обнаружения аномального поведения сетевого трафика показало его высокую эффективность.

КЛЮЧЕВЫЕ СЛОВА: псевдоградиентный алгоритм; условно нелинейная Парето – оптимальная фильтрация; нечеткий логический вывод Такаги–Сугено; нечеткая база правил; нечеткая база знаний.

Сведения об авторах:

[1]к.т.н., доцент, начальник научно-исследовательского отдела ОАО «Радиоавионика», г. Санкт-Петербург, Россия, serg123_61@mail.ru

[2]д.т.н., профессор, профессор Ульяновского государственного технического университета, г. Ульяновск, Россия, a_gladkikh@mail.ru

[3]д.т.н., профессор, заместитель генерального директора по научной работе АО «Научно-исследовательский институт «Рубин», г. Санкт-Петербург, Россия, vi-kurnosov@mail.ru

[4]д.в.н., профессор, профессор Петербургского государственного университета путей сообщения Императора Александра I, г. Санкт-Петербург, Россия, aprivalov@inbox.ru

Для цитирования: *Агеев С.А., Гладких А.А., Курносов В.И., Привалов А.А.* Адаптивный метод обнаружения аномалий трафика в высокоскоростных мультисервисных сетях связи // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 4–13. doi: 10.24411/2409-5419-2018-10282

Введение

Современный этап развития промышленности, бизнеса, транспортных и логистических систем, а также систем административного управления характеризуется успешным внедрением технологий высокоскоростных телекоммуникаций и сетей нового поколения (NGN). Достигнутые успехи в развитии технологий телекоммуникаций и связи привели к созданию и реализации концепции мультисервисной сети связи (МСС), ядром которой являются пакетные IP-сети, интегрирующие различные услуги передачи речи, данных и мультимедиа [1–2].

Основные сервисы, предоставляемые пользователям с помощью МСС, хорошо известны [2–3]. Однако появление большого количества дополнительных сервисов у МСС делает актуальной проблему надежного обеспечения ее сетевой и информационной безопасности (СИБ) [4].

Трафик в МСС является весьма разнообразным [3, 5–6]. Он состоит, в том числе, из мультимедийного трафика, который очень чувствителен к задержкам, трафика передачи данных, трафика передачи сигнальной информации, трафика электронной почты. При этом заданные требования к качеству сервисов должны выполняться полностью. Однако существуют объективные трудности в построении системы управления МСС и, в частности, в построении ее СИБ. Эти трудности вызваны сложностью структуры МСС, большим пространственным размахом сетевой инфраструктуры, необходимостью быстрого и качественного анализа большого количества различных динамично изменяющихся сетевых и информационных характеристик и параметров.

Следовательно, оперативное непрерывное оценивание и обнаружение аномального поведения высокоскоростного сетевого трафика с априори неизвестными, динамично изменяющимися характеристиками является одной из ключевых задач управления сетью МСС, а также ее СИБ, представляет собой актуальную научную проблему.

Анализ методов оценки характеристик и параметров трафика в высокоскоростных мультисервисных сетях связиСС

В работах [5–7] отмечается, что трафик для различных приложений в МСС может быть аппроксимирован с помощью вероятностных распределений, основными из которых являются распределение Пуассона, Парето, Вейбулла, логарифмически нормальное и экспоненциальное распределения.

Наиболее просто решить задачу оценивания текущих значений параметров трафика, если он является стационарным случайным процессом. Однако трафик в МСС является нестационарным по своей природе, а математические модели, адекватно описывающие его поведение, являются нелинейными стохастическими моделями [6–7]. Это обстоятельство существенно осложняет разработку и реализацию процедур оценки параметров и характеристик сетевого мультисервисного трафика с требуемым качеством в условиях априорной неопределенности как относительно его текущего вероятностного закона распределения, так и относительно его параметров.

Следует отметить, что основными характеристиками мультисервисного трафика являются максимальное и минимальное значение его интенсивности, текущее значение математического ожидания, среднее квадратичное отклонение и коэффициент вариации его интенсивности [6–7].

Одним из конструктивных подходов к решению задачи оценки векторных параметров случайных процессов, при нелинейных моделях наблюдений, является метод условной нелинейной Парето — оптимальной фильтрации [9–10]. Суть данного подхода заключается в том, что оценка векторного неизвестного параметра производится в два этапа. На первом этапе вычисляется функция текущего прогноза оценок значений векторного параметра. На втором этапе с помощью корректирующих функций и полученной дополнительной апостериорной информации о значениях этих оценок, производят их коррекцию. Выбор класса и вида функций оценки текущего прогноза, класса и вида корректирующих функций является достаточно свободным и определяется конкретной постановкой решаемой проблемы.

В данной работе, на основе условной нелинейной Парето — оптимальной фильтрации, разработаны метод и алгоритм обнаружения аномального поведения трафика, с использованием совместных оценок текущего значения математического ожидания, среднего квадратичного отклонения (СКО) и коэффициента вариации интенсивности трафика МСС. Предлагается адаптацию корректирующих функций к неизвестным характеристикам интенсивности трафика МСС производить с помощью псевдоградиентных процедур, общая теория которых была заложена в работах [10–12]. При этом регулирование параметров корректирующих функций в зависимости от параметров случайной последовательности (СП) производится с помощью нечеткого логического вывода Такаги-Сугено [14–15], с учетом динамики изменения их значений.

Формулировка проблемы, теоретические основы, метод и алгоритм оценки характеристик трафика в высокоскоростных мультисервисных сетях связи

Пусть наблюдения трафика МСС на соответствующем сетевом интерфейсе сетевого элемента, например, маршрутизатора, представлены в виде СП $x(i)$. Пусть СП $x(i)$ задана в дискретные моменты времени $t = t = \{1,2,\ldots, n, \ldots\}$. Пусть наблюдения СП $x(i)$ описываются аддитивно-мультипликативной моделью в виде:

$$x(i) \;=\; \theta(i)\times w\,(x(i\text{-}1)) \;+\; \xi(i),$$

где w (*) — некоторая случайная функция от наблюдений, $\theta(i)$ — некоторая случайная величина, а $\xi(i)$ — помеха наблюдений с нулевым математическим ожиданием и конечной дисперсией. Также пусть СП $x(i)$ имеет конечные математическое ожидание и дисперсию.

Необходимо построить векторную рекуррентную процедуру оценки значений математического ожидания СП $x(t)$, среднеквадратического отклонения СП и его коэффициента вариации по критерию минимума среднего квадрата ошибки, то есть необходимо обеспечить выполнения совместных условий:

$$\begin{aligned} J(i) = M\{\overline{\varepsilon}\} = \{M(m(i)-\hat{m}(i))^2\} \to \min, \\ M(\sigma(i)-\hat{\sigma}(i))^2 \;\to\; \min, \\ M(Kv(i)-\hat{K}v(i))^2 \;\to\; \min\}, \end{aligned} \tag{2}$$

где $\hat{m}(i)$, $\hat{\sigma}(i)$, $\hat{K}v(i)$ — оценки математического ожидания, СКО и коэффициента вариации СП $x(i)$ на шаге i, а $m(i)$, $\sigma(i)$, $K_v(i)$ — их истинные значения на этом шаге.

Функция прогноза для текущего значения математического ожидания СП определяется как:

$$\hat{m}(i) = \frac{1}{N}\sum_{k=1}^{N} x(i\text{-}k), \quad i = 1,\ 2,\ ...,\ n,\ ..., \tag{3}$$

где N — размер скользящего окна, который выбирается относительно небольшого размера [8].

Далее, прогнозы оценок СКО и коэффициента вариации СП на шаге i также производятся в этом же скользящем окне:

$$\begin{aligned} &\hat{\sigma}(i) = \sqrt{\frac{1}{N\text{-}1}\sum_{k=1}^{N} x^2(i\text{-}k) - \left(\frac{1}{N}\sum_{k=1}^{N} x(i\text{-}k)\right)^2}, \\ &i = 1,\ 2,\ ...,\ n, \\ &\hat{K}_V = \hat{\sigma}(i)\ /\ \hat{m}(i)\ , \end{aligned} \tag{4}$$

Без потери общности, дальнейшее подробное рассмотрение построения корректирующей процедуры проведем для компоненты значения оценки математического ожидания функционала (2), с последующим обобщением на векторный случай.

Значение функционала $J(\hat{m}(i))$ может быть недоступно наблюдению, а доступна наблюдению только случайная реализация его градиента со случайной ошибкой:

$$\nabla Q(\xi, \hat{m}(i)) = \nabla J(\hat{m}(i)) + \xi, \quad \xi \in R^n \tag{5}$$

где ξ — ошибка наблюдения градиента. Сделаем допущение о том, что ξ — центрированные, некоррелированные ошибки оценки градиента функционала качества. Минимизацию функционала (5) будем проводить с помощью рекуррентного алгоритма вида:

$$\hat{\hat{m}}(i+1) = \hat{\hat{m}}(i) - \lambda_m(i+1)\nabla Q(\xi,\ \hat{m}(i+1)), \tag{6}$$

где $\nabla Q(\xi,\ \hat{m}(i+1))$ — некоторое случайное направление движения в фазовом пространстве в точке $\hat{m}(i+1)$, $\hat{\hat{m}}(i)$ — скорректированная оценка математического ожидания на предыдущем шаге, $\{\lambda_m(i)\}$ — последовательность положительных чисел, которая для стационарного СП, должна удовлетворять условиям:

$$\sum_{i=1}^{\infty} \lambda_m(i) = \infty, \quad \sum_{i=1}^{\infty} \lambda_m^2(i) < \infty. \tag{8}$$

Эти числа называют коэффициентами шага алгоритма. В соответствии с [11–13] вектор $\nabla Q(\xi,\ \hat{m}(i))$ называется псевдоградиентом в точке $\hat{m}(i)$, если в этой точке выполняется условие:

$$\nabla J(\hat{m}(i-1)) \times M\{\nabla Q(\xi,\ \hat{m}(i))\} \geq 0, \tag{9}$$

где M(*) — операция математического ожидания, то есть, вектор $\nabla Q(\xi,\ \hat{m}(i))$ в среднем составляет острый угол с вектором градиента функционала качества $\nabla J(\hat{m}(i-1))$. Реализацию функционала качества в точке $\hat{m}(i+1)$, в соответствии с [8, 11–13], можно представить следующим образом:

$$Q(\hat{m}(i+1)) = (\hat{m}(i+1) - \hat{\hat{m}}(i))^2, \tag{10}$$

а его градиент в виде:

$$\begin{aligned} \Delta Q(\hat{m}(i+1)) &= \frac{\partial}{\partial\, \hat{y}(i)}\ (\hat{m}(i+1) - \hat{\hat{m}}(i))^2 = \\ &= -2\ (\hat{m}(i+1) - \hat{\hat{m}}(i)). \end{aligned} \tag{11}$$

Численный коэффициент в правой части полученного выражения можно учесть при выборе начального значения λ_m. Вид рекуррентного псевдоградиентного алгоритма (ПГА) оценивания текущего значения математического ожидания, с учётом знаков, будет иметь вид:

$$\hat{\hat{m}}(i+1)\ \hat{\hat{m}}(i) + \lambda_m(i+1)(\hat{m}(i+1) - \hat{\hat{m}}(i)). \tag{12}$$

Если плотность распределения значений СП $\hat{m}(i)\cdot p(\hat{m})$ симметрична относительно математического ожидания, то возможно применение ПГА вида:

$$\hat{\hat{m}}(i+1) = \hat{\hat{m}}(i) + \lambda_{i+1}\varphi(\hat{m}(i+1) - \hat{\hat{m}}(i)), \tag{13}$$

где в качестве функции φ(*) может быть использована неубывающая монотонная функция, например, знаковая функция φ(*) = sign(*). Применение данной функции позволяет повысить устойчивость ПГА к ошибкам оценки градиента функционала качества [11–13].

Обобщением алгоритма (12) является векторный ПГА оценки параметров СП, имеющий вид:

$$\hat{\bar{G}}(i+1) = \hat{\bar{G}}(i) + R(i+1) \times (\nabla \bar{Q}(i+1)), \qquad (14)$$

где $\hat{G}(i+1)$ — вектор оценок параметров СП на шаге $i + 1$, представимый в виде:

$$\hat{\bar{G}}(i+1) = [\hat{m}(i+1),\ \hat{\sigma}(i+1),\ \hat{K}_V(i+1)]^T. \qquad (15)$$

Матрица $R(i+1)$ является диагональной матрицей коэффициентов шага оцениваемых параметров.

Относительно алгоритмов (12), (13) и (14) можно сформулировать утверждения о том, что:

1. Данные алгоритмы являются псевдоградиентными алгоритмами. Доказательство данного утверждения основано на корректной проверке условия (9). Следствием из этого утверждения является то обстоятельство, что данные процедуры обладают всеми свойствами ПГА [11–13].

2. Структура алгоритмов (12) и (14) инвариантна относительно статистических характеристик СП $x(i)$, с точностью, определяемой точностью идентификации своих параметров. Доказательство данного утверждения основано на применении центральной предельной теоремы [6]. Следствием данного утверждения является то, что при любых вероятностных свойствах трафика, структура алгоритма оценки его параметров постоянна, изменяться могут только параметры его настройки.

Предлагаемая структура адаптивного алгоритма оценки параметров трафика МСС приведена на рис. 1.

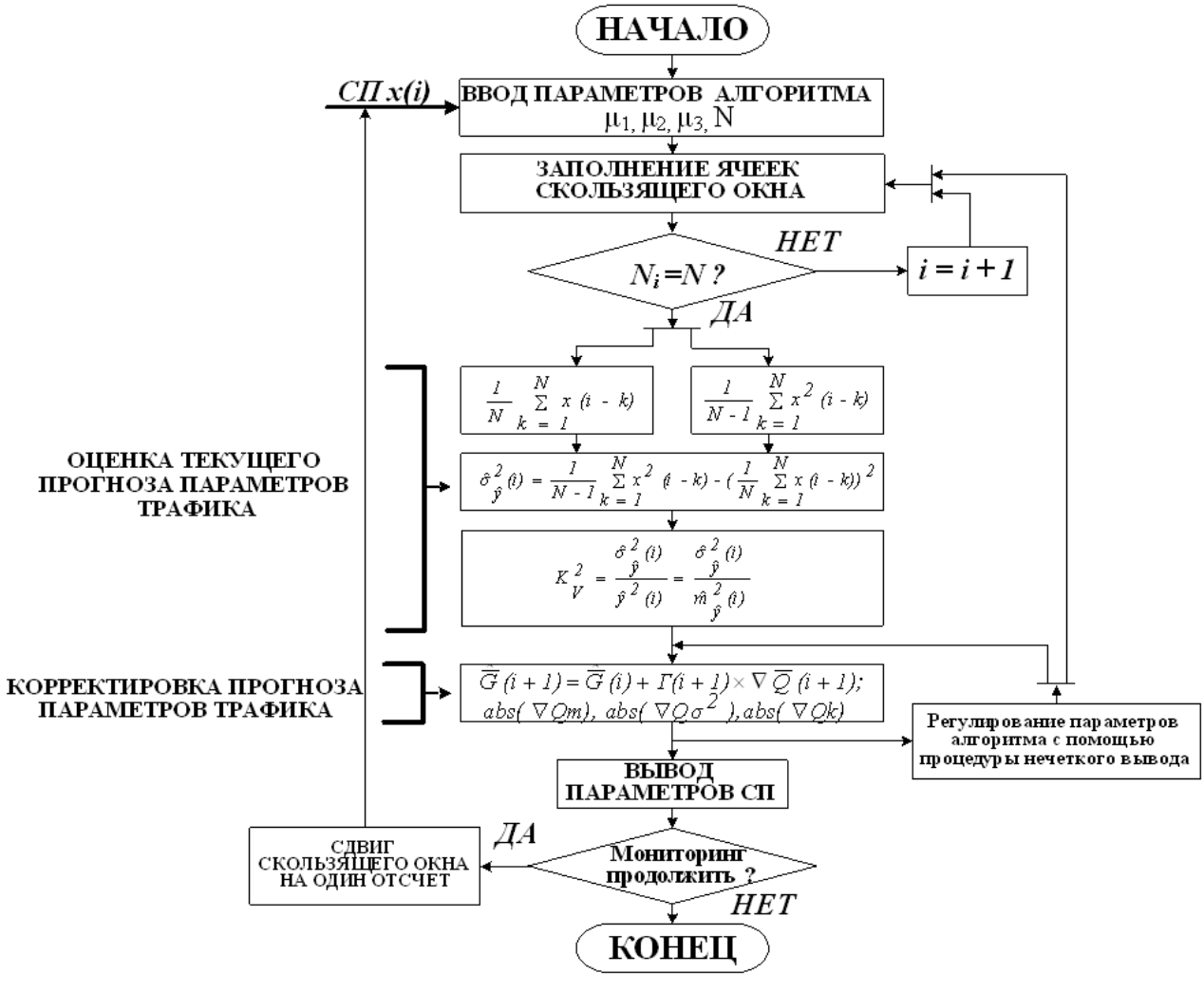


Рис. 1. Структура адаптивного алгоритма оценки параметров трафика МСС

Для оценивания параметров нестационарных СП условие (8) ограничивает применение ПГА, так как ПГА должен отслеживать изменения значения параметров трафика, а не сходиться к определённым их значениям. Поэтому предлагается последовательность $R(i+1)$ ограничить снизу постоянным значением. Как следствие выбора ограниченного коэффициента шага, дисперсия оценки параметров СП также будет ограничена снизу. Следовательно, необходимо найти компромиссное решение между скоростью и точностью оценивания значений интенсивности СП [8, 13].

В разработанных методе и алгоритме предлагается при выборе вектора коэффициентов шага учитывать динамику изменения оцениваемых параметров и характеристик СП.

Очевидно, что модули градиентов компонент векторного функционала качества пропорциональны динамическим свойствам СП. Подобные зависимости носят характер трудноформализуемых задач, поэтому предлагается процедуру подстройки коэффициентов шага ПГА автоматизировать на основе метода нечёткого вывода Такаги -Сугено или на основе его частного вида — синглтонного метода [14–15], имеющего вид:

Если

$$< \hat{G}(i) \in D1 > И < \nabla Q(i) \in D2 > B < \hat{\sigma}(i)) \in D3 > И < K_V \in U >,$$

$$\text{то } R\ (i+1) = R\ (z)\ И\ N = Nk \qquad (16)$$

Для реализации этих правил предварительно проводится обучение системы нечёткого логического вывода по экспериментальным данным, полученным на стадии ее проектирования, на тестовых СП, с известными статистическими параметрами [14–15]. Увеличение размера скользящего окна, если возникает такая необходимость, производится последовательно, с шагом равному одной ячейке скользящего окна. Это позволяет обеспечить наблюдаемость оцениваемых параметров СП.

Структура алгоритма обнаружения аномалий трафика МСС приведена на рис. 2. Здесь используются данные, полученные с помощью алгоритма оценки параметров трафика.

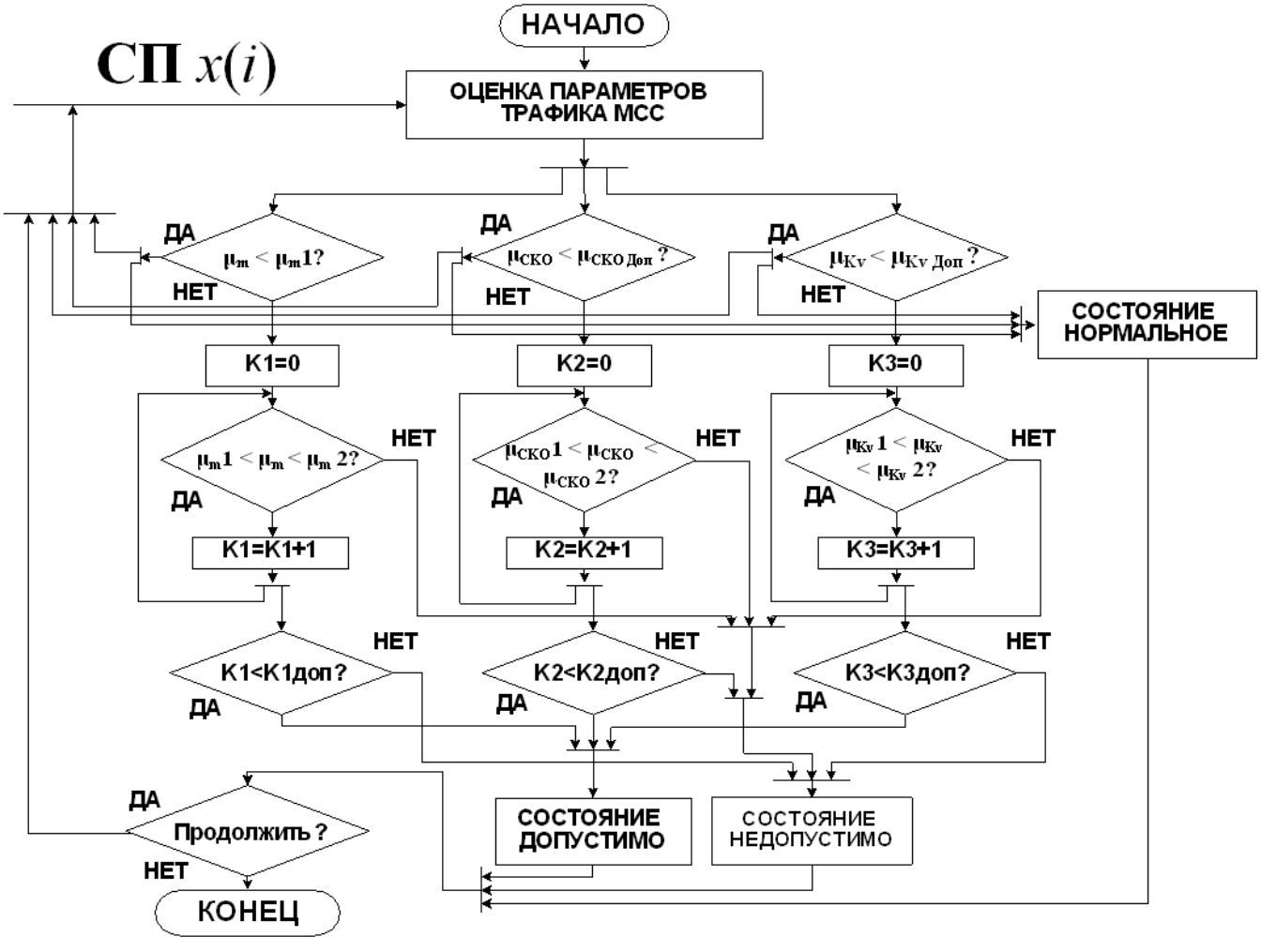


Рис. 2. Структура алгоритма обнаружения аномалий трафика МСС

Структура системы нечеткого логического вывода в процессе эксплуатации остается постоянной

Анализ результатов экспериментальной проверки

Математическое моделирование проверки эффективности разработанных алгоритмов оценки характеристик трафика МСС проводилось для трафиков имеющих распределение Пуассона, экспоненциальное распределение, логнормальное распределение и распределение Парето.

Модулирующие функции для моделирования нестационарных СП представляли собой СП авторегрессии первого порядка (АР-1), детерминированные периодические функции, ступенчатые функции.

На рис. 3 приведен полученный на этапе предварительного обучения системы нечеткого логического вывода график поверхности коэффициентов шага для процедуры корректировки оценок значений математического ожидания СП в зависимости от периода изменения математического ожидания СП и от возможного значения модуля оценки его градиента.

Обучение проводилось при заданном среднем значении СП равным $m_x(i) = 167$, коэффициенте вариации СП равным $K_V = 0{,}5$. По вертикальной оси λ_m выбран логарифмический масштаб. Аналогичные поверхности строятся и для других значений $m_x(i)$, количество которых определяется пропускной способностью канала связи с помощью эмпирически установленной зависимости — одна поверхность на один диапазон изменения математического ожидания равный $\Delta m_x(i) \approx 200$–$300$.

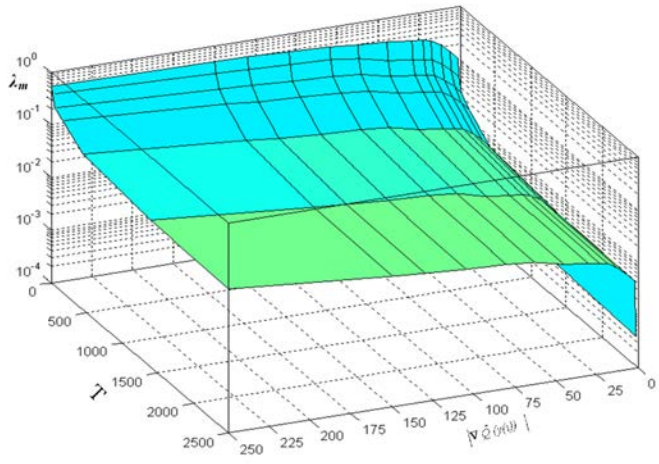
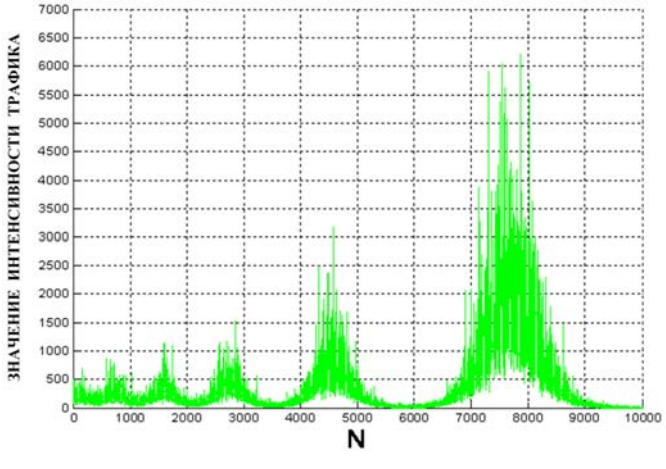


Рис. 3. Поверхность коэффициентов шага для процедуры корректировки оценки текущего значения математического ожидания СП, при $m_x(i) = 167$ и $K_V = 0{,}5$

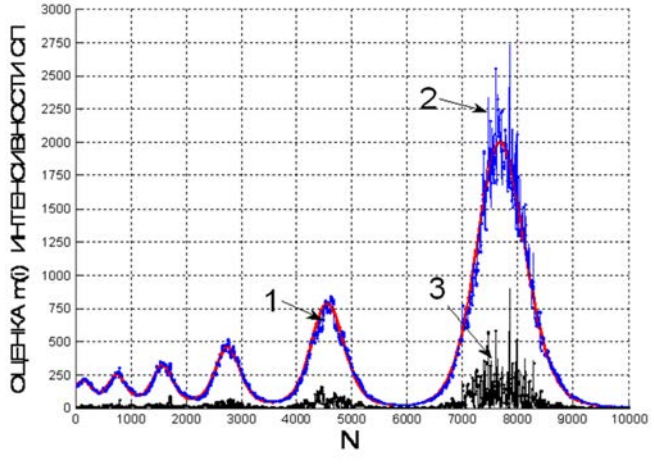
Следует отметить, что процедуры обучения системы нечеткого логического вывода достаточно легко автоматизируются.

В качестве примера, на рис. 4 приведены результаты оценки математического ожидания интенсивности трафика для изменяющейся амплитуды математического ожидания с одновременным увеличением периода его изменения для логарифмически нормального закона распределения.

Средняя относительная погрешность оценки математического ожидания составила менее 7,8 %.

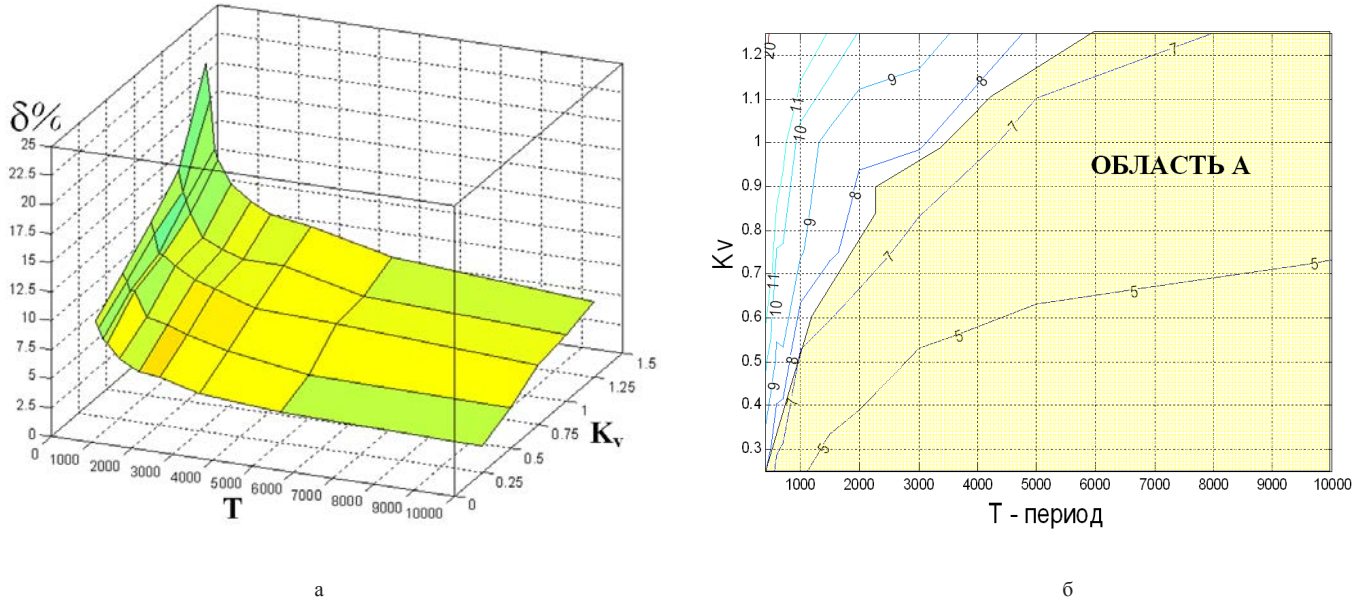


а



б

Рис. 4. Результаты оценки параметров нестационарного тренда с логарифмически нормальным распределением при изменяющихся параметрах интенсивности трафика: а) СП, б) результат оценки математического ожидания СП; 1 — истинное значение математического ожидания СП, 2 — оценка математического ожидания, 3 — модуль абсолютной погрешности оценки



а б

Рис. 5. а) Зависимость средней относительной погрешности оценки параметров СП в зависимости от скорости их изменения и от текущего значения коэффициента вариации; б) область А — область Парето оптимальных значений параметров алгоритма оценки параметров СП, в которой средние относительные погрешности оценок математического ожидания, СКО и K_V не превышает 9,4%

На рис. 5 представлены зависимости средней относительной погрешности оценки параметров СП в зависимости от скорости их изменения и от текущего значения коэффициента вариации при изменении математического ожидания от $m_x1(i)=167$ до $m_x2(i)=240$ и при изменении K_V от 0,25 до 1,25.

Область А на рис. 5 б) — область Парето — оптимальных значений параметров алгоритма оценки параметров СП, в которой средние относительные погрешности оценок математического ожидания, СКО и K_V не превышает 9,4%.

Пример обнаружения аномального поведения трафика с распределением Пуассона приведен на рис. 6. Математическое ожидание моделировалось процессом АР-1. Средняя относительная погрешность оценки составила $\delta \leq 1{,}7\%$. На данном рисунке зона А соответствует штатному поведению МСС, зона В — допустимому, а зона С — недопустимому состоянию МСС. Периодам времени Т1 и Т3 соответствуют недопустимые аномальные состояния трафика.

Пример аномального изменения среднеквадратического отклонения трафика для логнормального распределения приведен на рис. 7.

В этом эксперименте средняя относительная погрешность оценки математического ожидания не превысила 5,41%, средняя относительная погрешность оценки СКО не превысила 7,56%, средняя относительная погрешность оценки коэффициента вариации не превысила 7,1%. Значение абсолютного времени длительности аномального поведения трафика составило 2 млс.

Таким образом, разработанные метод и алгоритмы показали устойчивое детектирование аномального поведения трафика МСС в условиях высокой динамике изменения его характеристик с высокой точностью.

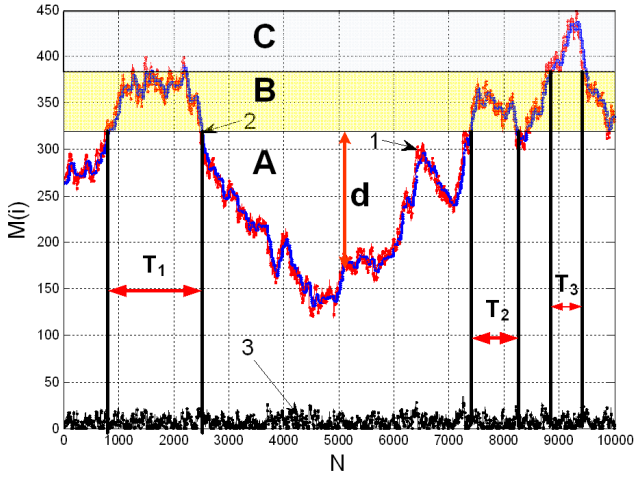


Рис. 6. Пример обнаружения аномального поведения трафика. Распределение Пуассона: 1 — истинное значение математического ожидания, 2 — значение его оценки, 3 — модуль ошибки оценивания

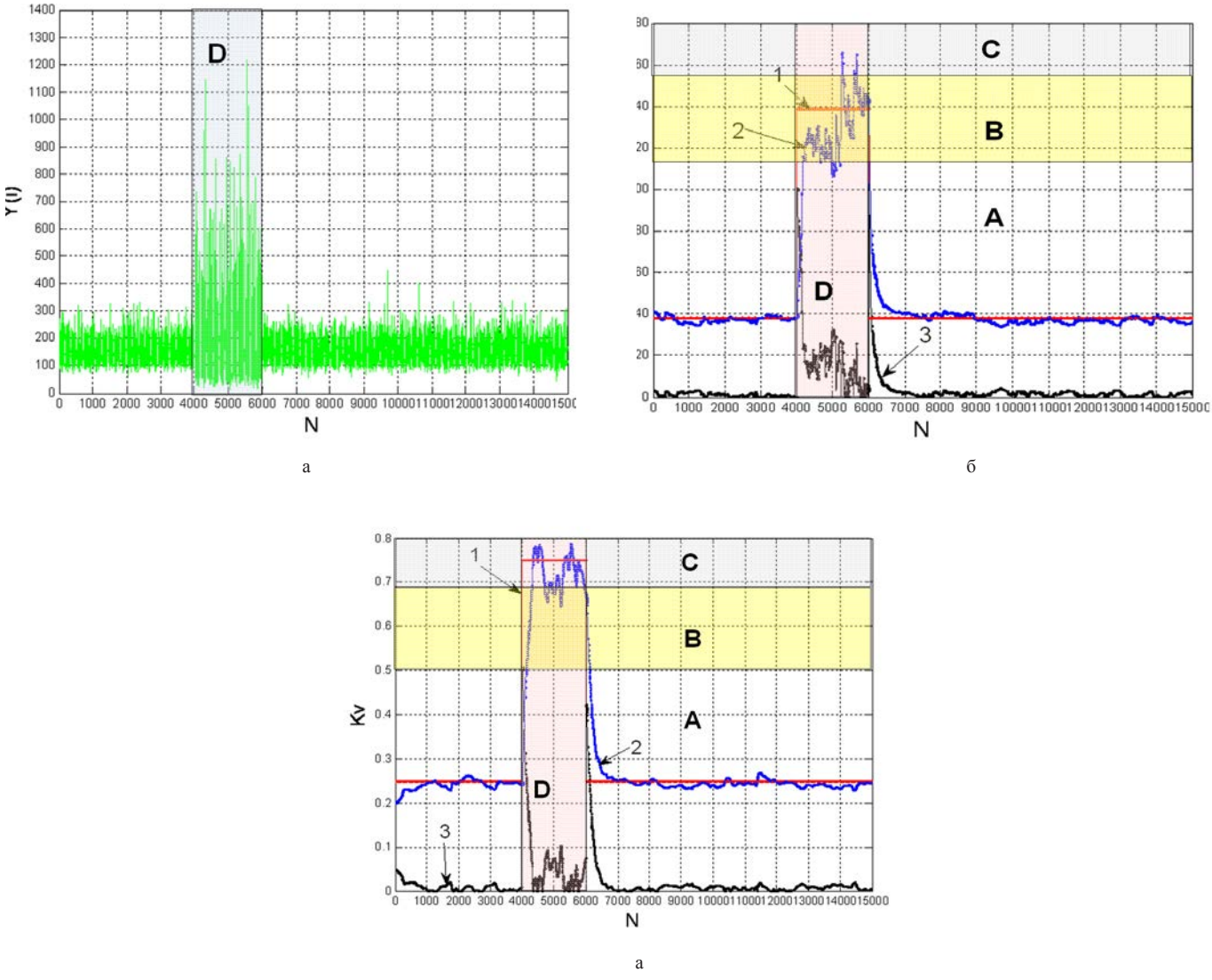


Рис. 7. Пример обнаружения аномального поведения трафика. Распределение логарифмически нормальное:
а) график СП, б) график СКО, 1 — истинное значение СКО, 2 — значение оценки СКО, 3 – модуль ошибки оценки;
в) график коэффициента вариации, 1 — истинное значение *Kv*, 2 — значение оценки *Kv*,
3 — модуль ошибки оценки. Зона D на всех графиках соответствует аномалии

Заключение

Полученные точностные и динамические характеристики разработанных метода и алгоритма обеспечивают обнаружение аномального поведения трафика МСС в высокоскоростных мультисервисных сетях связи с требуемым качеством.

Проведенный предварительный в работе анализ показал возможность аппаратно-программной реализации разработанных алгоритмов на существующей аппаратной платформе [16–18].

Наиболее перспективной является реализация алгоритма как интеллектуального агента для многоагентной интеллектуальной системы оперативной поддержки принятия решений. Аппаратной основой подобной системы может быть система на кристалле (SoC) и ПЛИС (FPGA).

Литература

1. ITU-T Recommendation Y.2001. General overview of NGN. Geneva, 2004. 18 p.

2. ITU-T Recommendation G.1000. Communications quality of service: A framework and definitions. 2001. 16 p.

3. *Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г.* Сети связи. СПб: БХВ Санкт-Петербург, 2011. 400 с.

4. ISO/IEC27001:2005. Information technology. Security techniques. Information security management Systems. Requirements. 2005. 34 p.

5. Симонина О. А. Модели расчета показателей QoS в сетях следующего поколения: дис. … канд. техн. наук. СПб.: 2005. 132 с.

6. *Шелухин О. И., Осин А. В., Смольский С. М.* Самоподобие и фракталы. Телекоммуникационные приложения. М.: Физматлит, 2008. 368 с.

7. *Шелухин О. И., Сакалема Д. Ж., Филинова А. С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии) / Под ред. профессора О. И. Шелухина. М.: Горячая линия — Телеком, 2013. 220 с.

8. *Агеев С. А., Саенко И. Б., Котенко И. В.* Метод и алгоритмы обнаружения аномалий в трафике мультисервисных сетей связи, основанные на нечетком логическом выводе // Информационно-управляющие системы. 2018. № 3. С. 61–68. doi:10.15217/issn1684–8853.2018.3.61.

9. *Пугачев В. С.* Обобщение теории условно оптимального оценивания и экстраполяции // Докл. АН СССР. 1982. Т. 262. № 3. С. 535–538.

10. *Пугачев В. С.* Условно оптимальная фильтрация и экстраполяция непрерывных процессов // Автоматика и телемеханика. 1984. № 2. С. 82–89.

11. *Поляк Б. Т., Цыпкин Я. З.* Псевдоградиентные алгоритмы адаптации и обучения // Автоматика и телемеханика. 1973. № 3. С. 45–63.

12. *Поляк Б. Т., Цыпкин Я. З.* Оптимальные псевдоградиентные алгоритмы адаптации // Автоматика и телемеханика. 1980. № 8. С. 74–84.

13. *Граничин О. Н.* Рандомизированные алгоритмы оптимизации и оценивания при почти произвольных помехах. М.: Наука, 2003. 291 с.

14. *Takagi T., Sugeno M.* Fuzzy Identification of Systems and Its Applications to Modeling and Control // IEEE Transactions on systems, man, and cybernetics. 1985.Vol. SMC-15. No.1. Pp. 116–132.

15. *Пегат А.* Нечеткое моделирование и управление: пер. с англ. М.: БИНОМ Лаборатория знаний, 2013. 798 с.

16. Intel. URL: https://www.intel.com/content/www/us/en/products/programmable.html (дата обращения 10.06.2019).

17. Xilinx. URL: http:// www.xilinx.com (дата обращения 10.06.2019).

18. OpenCores. URL: http://opencores.org/projects (дата обращения 10.06.2019).

ADAPTIVE METHOD OF DETECTING TRAFFIC ANOMALIES IN HIGH-SPEED MULTISERVICE COMMUNICATION NETWORKS

SERGEY A. AGEEV
St-Petersburg, Russia, serg123_61@mail.ru

ANATOLY A. GLADKIKH
Ulyanovsk, Russia, a_gladkikh@mail.ru

VALERY I. KURNOSOV
St-Petersburg, Russia, vi-kurnosov@mail.ru

ANDREY A. PRIVALOV
St-Petersburg, Russia, aprivalov@inbox.ru

KEYWORDS: pseudogradient procedures; notionally nonlinear Pareto – optimal filtering; Takagi-Sugeno fuzzy logical inference method; fuzzy rule base; fuzzy knowledge base.

ABSTRACT

In the work we present and research an adaptive heuristic (behavioral) method of detecting traffic anomalies in high-speed multi-service communication networks, functioning in real time. The actual of this study due to the fact that many processes of information and network security management, as well as processes of risk management of their threats realization in high-speed multi-service communication networks need to be implemented in close to real time. The approach proposed in the work is based on the concept of conditional nonlinear Pareto - optimal filtration by V. S. Pugachev. The main idea of this approach is that the traffic parameter is estimated in two stages, at the first stage the forecast of parameter values is estimated, and at the second stage the following observations of

parameters are obtained, their values are corrected. In the proposed method and algorithm, traffic parameter values are predicted in a small sliding window, and adaptation is implemented on the basis of pseudogradient procedures, parameters of which are adjusted by means of the Takagi-Sugeno fuzzy logical inference method. A feature of the developed procedures for estimating characteristics high-speed traffic of multi-service communication networks is that they allow to take into account dynamics change parameters of network traffic. The proposed method and algorithm belong to a class of adaptive methods and algorithms with pre-learning. Average relative error of estimated traffic parameters estimation does not exceed 10%, which is sufficient value for implementation of operational network control tasks. The procedure of detecting abnormal traffic behavior of the high-speed multi-service communication network in operation is implemented on the basis of the Mamdani fuzzy logic inference method, in which intervals of traffic parameters state are determined on the basis of the adopted security policy in the network. The study of the proposed method of detecting abnormal behavior of network traffic showed its high efficiency.

REFERENCES

1. ITU-T Recommendation Y.2001. General overview of NGN. Geneva, 2004. 18 p.

2.ITU-T Recommendation G.1000. Communications quality of service: A framework and definitions. Geneva, 2001. 16 p.

3. Gol'dshtejn B.S., Sokolov N.A., Janovskij G.G. *Setisvjazi* [Telecommunication Networks]. St. Petersburg: BHV St. Petersburg, 2011. 400 p. (In Russian).

4. ISO/IEC27001:2005. Information technology. Security techniques. Information security management Systems. Requirements. 2005. 34 p.

5. Simonina O.A. *Modeli rascheta pokazateley QoS v setyakh sleduyushchego pokoleniya* [Models of calculation of indicators Qosv networks of the next generation: dis. … candidate of technical Sciences]. St. Petersburg, 2005. 132 p. (In Russian)

6. Sheluhin O.I., Osin A.V., Smol'skij S.M. *Samopodobie I fraktaly. Telekommunikacionnye prilozhenija* [Self-similarity and fractals. Telecommunication application]. Moscow: Fizmatlit Publ., 2008. 368 p. (In Russian)

7. Sheluhin O.I., Sakalema D. Zh., Filinova A.S. *Obnaruzhenie vtorzhenij v komp'juternye seti (setevye anomalii)* [Intrusion detection in computer networks (network anomalies)]. Moscow: Goryachaya liniya – Telekom, 2013. 220 p. (In Russian)

8. Ageev S.A., Saenko I.B., Kotenko I.V. Method and Algorithms of Anomaly Detection in Multiservice Network Traffic based on Fuzzy Logical Inference. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems]. 2018. No. 3. Pp. 61–68. doi:10.15217/issn1684–8853.2018.3.61 (In Russian)

9. Pugachev V.S. Obobshchenie teorii uslovno optimal'nogo ocenivaniya I ekstrapolyacii [Generalization of the theory of conditionally optimal estimation and extrapolation]. *Doklady AN SSSR* [Report at an Academy of Sciences of the USSR]. 1982. T. 262. No. 3. Pp. 535–538. (In Russian)

10. Pugachev V.S. onditionally optimal filtering and extrapolation of continuous processes. *Automation and Remote Control.* 1984. Vol. 45. No. 2. Pp. 212–218.

11. Polyak B.T., Tsypkin Ja.Z. Pseudogradient adaptation and learning algorithms. *Automation and Remote Control*. 1973. Vol. 34. No. 3. Pp. 377–397.

12. Polyak B.T., Tsypkin Ja.Z. Optimal pseudogradient adaptation algorithms. *Automation and Remote Control.* 1980. Vol. 41. No. 8. Pp. 1101–1110.

13. Granichin O.N. *Randomizirovannye algoritmy optimizacii I ocenivanija pri pocht iproizvol'nyh pomehah* [Randomized algorithms of optimization and estimation in case of almost arbitrary interference]. Moscow: Nauka, 2003. 291 p. (In Russian)

14. Takagi, T., Sugeno, M.: Fuzzy Identification of Systems and Its Applications to Modeling and Control. *IEEE Transactions on systems, man, and cybernetics*. 1985. Vol. SMC-15. No.1. Pp. 116–132.

15. Piegat A. *Fuzzy Modeling and Control.* New York: Physica-Verl., 2001. 712 p.

16. Intel. URL: https://www.intel.com/content/www/us/en/products/programmable.html (date of access 10.06.2019).

17. Xilinx. URL: http:// www.xilinx.com (date of access10.06.2019).

18. OpenCores. URL: http://opencores.org/projects (date of access 10.06.2019).

INFORMATION ABOUT AUTHORS:

Ageev S.A., PhD, Docent, Head of Department of the Radioavionica JSC.

Gladkikh A.A., PhD, Full Professor, Professor of the Ulyanovsk State Technical University.

Kurnosov V.I., PhD, Full Professor, Deputy General Director of JSC "Research Institute "Pubin".

Privalov A.A., PhD, Full Professor, Professor of the Emperor Alexander I St. Petersburg State Transport University.

For citation: Ageev S.A., Gladkikh A.A., Kurnosov V.I., Privalov A.A. Adaptive method of detecting traffic anomalies in high-speed multiservice communication networks. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 4–13. doi: 10.24411/2409-5419-2018-10282 (In Russian)

doi: 10.24411/2409-5419-2018-10283

ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ ПРОЦЕССА ОПЕРАТИВНОГО ВОССТАНОВЛЕНИЯ ИЗДЕЛИЙ СЛОЖНЫХ ТЕХНИЧЕСКИХ КОМПЛЕКСОВ В ВИДЕ ДЕСКРИПТИВНОЙ МОДЕЛИ

АНИСИМОВ
Олег Витальевич[1]

КУРЧИДИС
Виктор Александрович[2]

КОРОБКО
Вадим Александрович[3]

АННОТАЦИЯ

Рассматривается процесс оперативного восстановления изделий сложных технических комплексов с точки зрения его модельного представления, предназначенного для использования в средствах автоматизации деятельности личного состава дежурной смены центра ситуационного управления работами по ремонту и сервисному обслуживанию. Предлагается сокращение времени формирования оперативной информации за счет перехода к формализованному представлению этого процесса. Представлены ограничения существующих модельных представлений рассматриваемого процесса, используемых в средствах автоматизации этого центра. Имеющиеся ограничения приводят к необходимости многократной взаимной интерпретации данных и предметных понятий процесса оперативного восстановления в деятельности личного состава дежурной смены центра ситуационного управления, что негативно отражается на времени оперативного восстановления изделий сложных технических комплексов. Предлагается логико-лингвистический подход к формализации модельного представления такого процесса, который расширяет возможности существующих моделей и позволяет формализовать смысловые связи между элементами процесса оперативного восстановления в понятиях и терминах естественного языка. Предлагаемое формализованное представление процесса относится к классу дескриптивных моделей и ориентируется на сочетание логического описания этого процесса с его описанием на естественном языке. Рассмотренный подход способствует определению требований к оперативной информации в предметных понятиях и терминах естественного языка. Это снижает непроизводительные временные затраты на формирование оперативной информации. Использование предлагаемой дескриптивной модели в средствах автоматизации центра ситуационного управления направлено на уменьшение времени оперативного восстановления изделий сложных технических комплексов за счет сокращения времени формирования оперативной информации в деятельности личного состава дежурной смены.

КЛЮЧЕВЫЕ СЛОВА: оперативное восстановление; информационная поддержка; дескриптивная модель; дескриптивные элементы представления процесса; автоматизация.

Сведения об авторах:

[1]д.т.н., доцент, профессор Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, qwaker@inbox.ru

[2]д.т.н., профессор, профессор Ярославское высшее военное училище противовоздушной обороны, г. Ярославль, Россия, idahmer2@yandex.ru

[3]адъюнкт Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, vadym.korobko@yandex.ru

Для цитирования: *Анисимов О.В., Курчидис В.А., Коробко В.А.* Формализованное представление процесса оперативного восстановления изделий сложных технических комплексов в виде дескриптивной модели // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 14–21. doi: 10.24411/2409-5419-2018-10283

Введение

Оперативное восстановление изделий сложных технических комплексов (СТК) представляет собой процесс, определяющий общую организацию деятельности по дефектации и войсковому ремонту компонентов таких изделий в местах размещения [7–9]. Этот процесс проводится с участием различных групп лиц (личный состав эксплуатирующих подразделений, представители сервисных служб предприятий промышленности и т. д.), а его выполнение характеризуется необходимостью учета большого числа объективных и субъективных факторов в соответствии с общим порядком выполнения ремонта и технического обслуживания комплексов, определяемым нормативными документами. К таким факторам относятся: количество изделий сложных технических комплексов, их пространственная распределенность по территории РФ, техническое состояние изделий СТК, контрактная система работ, количество и состав выездных ремонтных бригад и т. п.

Для оперативной работы с информацией, определяемой перечисленными выше факторами, используются средства автоматизации информационной поддержки Центра ситуационного управления (ЦСУ) АО «ГПТП «Гранит», которые являются составной частью интегрированной автоматизированной системы управления жизненным циклом (ИАСУ ЦСУ) изделий СТК, создаваемых на предприятиях АО «Концерн ВКО «Алмаз — Антей». При этом деятельность по оперативному восстановлению изделий СТК организуется личным составом дежурной смены этого центра.

Временной анализ процесса оперативного восстановления изделий СТК показывает, что этот процесс характеризуется возможностью многократного повторения определенных действий по дефектации и войсковому ремонту до приведения этих изделий в работоспособное состояние [2] в рамках цикла оперативного восстановления. Декомпозиция каждого из этих действий обеспечивает представление процесса оперативного восстановления изделий СТК в виде совокупности операций, выступающих в качестве структурообразующих единиц этого процесса.

Каждая из операций процесса оперативного восстановления изделий СТК связана с формированием и использованием личным составом дежурной смены ЦСУ разнородной оперативной информации. При этом участие личного состава дежурной смены в этих операциях характеризуется высоким уровнем неопределенности, многоальтернативностью принимаемых решений и многократным использованием различных сведений, содержащихся в базе данных (БД) ИАСУ ЦСУ, для формирования разнообразной оперативной информации: об отказавшем изделии СТК (наименование или маркировка изделия, место дислокации), об отказе (характер отказа, возможности восстановления силами обслуживающего персонала, возможность восстановления силами ремонтных подразделений, необходимость привлечения ремонтных бригад), об имеющихся ресурсах (наличие запасных частей и принадлежностей, ремонтного оборудования, ремонтного персонала), о возможных вариантах проведения работ (на местах эксплуатации или в заводских условиях), о наличии оснований на проведение работ (по гарантии, по истечении гарантии), о состоянии работ (наличие документов на работы, состав ремонтных бригад и маршруты их следования) и т. п. Время на формирование этой информации является составной частью общих временных затрат на выполнение операций по оперативному восстановлению и в значительной степени определяет значение общего времени восстановления изделий СТК.

Алгоритмические средства ИАСУ ЦСУ основаны на запросно-ответных механизмах, определяющих требования к необходимой оперативной информации с помощью традиционных средств указания либо с помощью языковых средств командной строки. Однако, как показано в работах [4, 14], запросно-ответные механизмы, используемые в средствах автоматизации ИАСУ ЦСУ, характеризуется высокой долей ручных операций, связанных с выполнением различных манипуляций при формировании запросов, что ограничивает возможности таких средств по сокращению времени формирования оперативной информации в цикле оперативного восстановления.

Существующие средства автоматизации информационной поддержки операций процесса ОВ изделий СТК основываются на формальном представлении этого процесса, как сложноорганизованной деятельности. Известные подходы к формальному описанию процессов деятельности базируются на принципе многомодельности [13], основанном на утверждении о том, что никакая единственная модель не может с достаточной степенью адекватности описывать различные аспекты сложной системы или процесса. Применительно к процессу оперативного восстановления это означает, что достаточно полная модель этого процесса образуется посредством объединения некоторого число взаимосвязанных представлений, каждое из которых адекватно отражает некоторый аспект описания этого процесса.

В настоящее время для формализованного описания процесса оперативного восстановления, как процесса деятельности используются методологии IDEF0, IDEF3, DFD, UML и т. п. [1, 3, 5, 10–13]. Такие методологии базируются на многоаспектном представлении процесса, и основу этого представления образует структурный, функциональный, временной и ресурсный аспект, а также аспект потоков данных. Представление каждого из этих аспектов связывается с разработкой и использованием совокупности частных формализованных моделей, интеграция ко-

торых обеспечивает единое формальное представление процесса.

В целом использование известных методологий для процесса ОВ изделий СТК позволяет формировать модели, сочетающие графическое и вербальное представление различных аспектов деятельности в рамках этого процесса. Так, использование модели, создаваемой на основе методологии функционального моделирования IDEF0 [3, 10–11], позволяет графически представлять структуру и функции процесса ОВ изделий СТК, а также потоки информации и материальных объектов, связывающие операции этого процесса. Использование модели, создаваемой по методологии потоков данных DFD [1, 11–12], обеспечивает графическое описание внешних по отношению к рассматриваемому процессу функций, источников и потребителей данных, а также информационные потоки и хранилища данных. В целом использование таких моделей обеспечивает достаточно подробное модельное представление процесса ОВ изделий СТК, которое находит отражение в инфологической модели базы данных и алгоритмических средствах ИАСУ ЦСУ, образующих основу средств автоматизации информационной поддержки личного состава дежурной смены Центра ситуационного управления АО «ГПТП «Гранит».

Однако семантические связи, присутствующие в этих моделях, не находят своего отражения в средствах автоматизации ИАСУ ЦСУ, что в деятельности личного состава дежурной смены приводит в необходимости многократной взаимной интерпретации данных и предметных понятий и терминов, используемых в описании процесса P оперативного восстановления изделий СТК. Вследствие этого временные затраты, связанные с формированием и использованием оперативной информации при выполнении операций оперативного восстановления изделий СТК, являются значительными.

Сокращение времени оперативного восстановления изделий СТК в данной работе связывается с переходом к формализованной модели $L(P)$, которая расширяет возможности существующих моделей и позволяет формализовать смысловые связи между элементами процесса P оперативного восстановления в понятиях и терминах естественного языка. Такая модель относится к классу дескриптивных, и в данной работе она ориентируется на сочетание логического и лингвистического описания процесса оперативного восстановления для обеспечения возможности формализованного описания операций процесса и взаимосвязей между ними на естественном языке. В целом это связывается с предоставлением возможности формально определять требования к необходимой оперативной информации в запросах к ИАСУ ЦСУ с использованием естественно-подобного языка. Реализация такой возможности в существующих средствах автоматизации ИАСУ ЦСУ направлена на сокращение времени оперативного восстановления за счет уменьшения времени формирования необходимой оперативной информации.

Структура формализованного представления процесса оперативного восстановления изделий сложных технических комплексов

Вопросы построения и использования формализованной модели $L(P)$ для процесса оперативного восстановления изделий СТК в литературе отсутствуют, что приводит к необходимости решения научной задачи по созданию такой модели. Решение этой задачи предлагается выполнить на основе логико-лингвистического подхода [6] за счет формализации семантического и языкового представления процесса ОВ изделий СТК. Такой подход предлагается реализовать на основе моделей, создаваемых в рамках существующих методологий IDEF и DFD, обеспечивающих многоаспектную декомпозицию процесса оперативного восстановления изделий СТК. При этом в качестве математической основы выступает формальный аппарат дескриптивной логики [15–16].

Анализ процесса оперативного восстановления изделий СТК показывает, что при многоаспектном представления этого процесса целесообразно учитывать следующие аспекты η: структурный ($\eta = S$), функциональный ($\eta = F$), временной ($\eta = T$), ресурсный ($\eta = U$), а также аспект представления данных ($\eta = W$). Для любого из этих аспектов предлагается выделять процессные элементы и взаимосвязи между ними, которые представляются в предметных понятиях и терминах естественного языка. Процессными элементами для процесса ОВ изделий СТК являются различные информационные и материальные объекты, участвующие в деятельности по реализации этого процесса. В качестве таких элементов в процессе ОВ изделий СТК могут выступать операции, документы, ресурсы и т. п., которые представляются в существующих моделях (IDEF0, DFD и т. д.) процесса соответствующими предметными понятиями. При этом взаимосвязи между элементами процесса представляются отношениями, выражаемыми на естественном языке, такими, как, например, «выполняется до», «выполняется после», «зависит от», «влияет на» и т. п.

С логико-лингвистической точки зрения представление $L_\eta(P)$ всякого рассматриваемого выше η-го аспекта процесса P, $\eta \in \{S, F, U, T, W\}$, основывается на том, что формально необходимо учитывать два представления всякого аспекта — теоретико-множественное в виде модели $L^1_\eta(P)$ и вербальное в виде модели $L^2_\eta(P)$. Это определяет общую структуру формализованного представления рассматриваемого процесса оперативного восстановления в следующем виде:

$$L_\eta(P) = L_\eta\left(L^1_\eta(P), L^2_\eta(P)\right) \quad (1)$$

Модель $L^1_\eta(P)$ в теоретико-множественной форме определяет и связывает процессные элементы, характеризующие всякий η-й аспект представления процесса *P*. Модель $L^2_\eta(P)$ в вербальной форме определяет в предметных понятиях и терминах естественного языка процессные элементы и связи между ними, определенные в модели $L^1_\eta(P)$.

Теоретико-множественное представление аспектов процесса оперативного восстановления изделий СТК

Теоретико-множественное представление всякого аспекта η процесса *P* определяется путем выделения соответствующих процессных элементов Θ_η, а также связей Cη между ними, так, что формально η-й аспект представления процесса оперативного восстановления может быть записан в следующем виде:

$$L^1_\eta(P) = \left\{\Theta_\eta, C_\eta\left(\Theta_\eta\right)\right\} \quad (2)$$

Так, например, теоретико-множественное представление структурного аспекта $L^1_S(P)$ процесса $P(\eta = S)$ связывается с выделением структурных процессных элементов, в качестве которых выступают операции *O*, так, что $O = \Theta_S$. Определение соответствующих структурных связей $C_S(O)$ основывается на том, что всякий процесс имеет входы и выходы. Выделение таких связей позволяет отражать порядок выполнения операций в процессе *P* и их иерархию. Формально структурный аспект процесса оперативного восстановления целесообразно представить в следующем виде:

$$L^1_S(P) = \left\{O, C_S(O)\right\} \quad (3)$$

где $O = \{o_1, o_2, \ldots\}$ — множество операций процесса *P* оперативного восстановления изделий СТК,

$C_S(O) = \{c_{s1}, o_{s2}, \ldots\}$ — множество структурных связей между операциями процесса оперативного восстановления изделий СТК.

Формально всякую структурную связь $c_s \in C_S$ в процессе *P* целесообразно представить в виде упорядоченной пары вида $c_s = c_s\langle o', o''\rangle \ \ (o', o'' \in O)$,

где o′ — операция, предшествующая операции o″ как представлено на рис.

Использование структурных связей позволяет всякую операцию $o_i \in O$ процесса оперативного восстановления формально представить в следующем виде:

$$o_i = o\left(C^+_{si}, C^-_{si}\right). \quad C^+_{si}, C^-_{si} \subseteq C_S \quad (4)$$

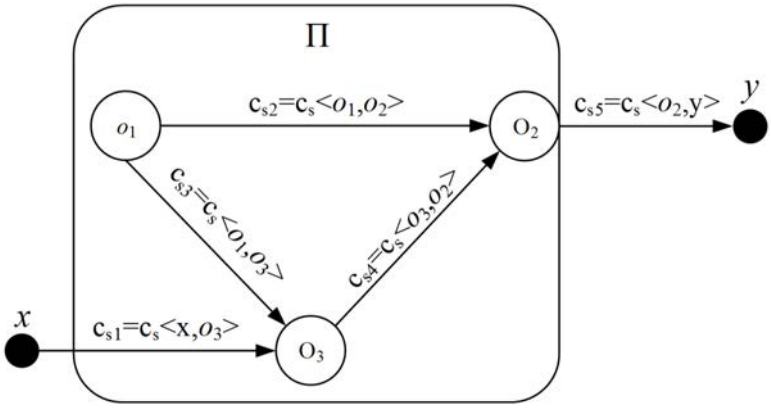
где C^+_{si} — множество структурных связей по входу для операции $o_i \in O$,

C^-_{si} — множество структурных связей по выходу для операции $o_i \in O$.

Теоретико-множественное представление других аспектов процесса оперативного восстановления изделий СТК, характеризуется использованием соответствующих процессных элементов и видов связей.

Вербальное представление аспектов процесса оперативного восстановления изделий СТК

Вербальное представление всякого η-го аспекта процесса *P* связано с определением в предметных понятиях и терминах естественного языка процессных элементов и связей между ними, представленных в соответствующей модели $L^1_\eta(P)$. При этом необходимо учитывать две стороны вербального представления процесса ОВ изделий СТК. С одной стороны, необходимо иметь в виду наличие



Графическое представление структурного аспекта процесса оперативного восстановления изделий вооружения и военной техники противовоздушной обороны с теоретико-множественной точки зрения

понятий и терминов естественного языка, используемых при выполнении теоретико-множественного представления η-го аспекта процесса ОВ изделий СТК. С другой стороны, необходимо учитывать понятия и термины естественного языка, определяющие предметное описание η-го аспекта процесса оперативного восстановления ОВ изделий СТК.

В соответствии с этим процессные элементы Θ_η оперативного восстановления изделий СТК предлагается рассматривать с предметной и прикладной точек зрения. Для этого целесообразно определять процессные элементы (ЭП) двух видов: первого — ЭП1 и второго — ЭП2 вида. Элементы ЭП1 определяют классы, образованные видами элементов, используемыми в модели $L^1_\eta(P)$ и представляемыми соответствующими понятиями, такими, как, например, «операция», «документ», «уведомление», «представитель заказчика». Элементы ЭП2 представляют собой экземпляры классов элементов первого вида с конкретными свойствами и характеристиками, например, «рекламационный акт на изделие И1», «представитель ГПТП «Гранит» ФИО».

Смысловые содержание взаимосвязей $C_\eta(\Theta_\eta)$ между всякими процессными элементами Θ_η вербально предлагается определять на основе отношений, представляемых в понятиях естественного языка. Примерами таких отношения являются: «влияет на», «используется», «зависит от» и т. п.

В соответствии с определенным вербальным представлением процессных элементов и взаимосвязей между ними формально логику деятельности личного состава дежурной смены ЦСУ предлагается отражать на основе дескриптивных элементов представления процесса (ДЭП). Всякий ДЭП предлагается представлять на основе триплетных предикатных структур (триплетов) ψ вида $\alpha r \beta$, где α и β определяют процессные элементы в понятиях и терминах естественного языка, а отношение *r* отражает семантическое (смысловое) содержание связи между α и β, также в терминах естественного языка. Наличие двух видов элементов процесса (ЭП1 и ЭП2) определяет два вида дескриптивных элементов представления процесса: ДЭП1 (ψ_1) и ДЭП2 (ψ_2). Дескриптивные элементы ψ_1 характеризуются тем, что в них в качестве α и β вступают элементы ЭП1, а элементы ψ_2 — тем, что в них в качестве α и β вступают элементы ЭП2. При этом элементы ψ_2 определяются на основе ψ_1, так, что с каждым элементом ψ_1 может быть связано множество $\Psi(\psi_1)$ элементов ψ_2. Тогда формальное вербальное представление η-го аспекта процесса *P*, соответствующее теоретико-множественному представлению $L^1_\eta(P)$, определяется в виде следующей дескриптивной модели, образованной совокупностью дескриптивных элементов второго вида:

$$L^2_\eta(P) = \bigcup_{i=1}^{i=N_\eta} \Psi\left(\psi^i_{1\eta}\right) \quad (5)$$

где N_η — общее количество процессных элементов в множестве Θ_η.

В соответствии с необходимостью учета всех аспектов процесс *P* оперативного восстановления изделий СТК предлагается формально представить в виде дескриптивной модели $L = L(P)$, являющейся совокупностью дескриптивных представлений каждого из аспектов:

$$L(P) = \bigcup_{\eta\in\{S,F,U,T,W\}} L^2_\eta(P) \quad (6)$$

Правая часть этого выражения показывает, что модель *L*(*P*) определяется совокупностью дескриптивных представлений структурного, функционального, ресурсного и временного аспекта, а также аспекта данных процесса *P*. Формализация каждого из аспектов и формирование соответствующих дескриптивных представления процесса ОВ изделий СТК является самостоятельной задачей. При этом построение общей дескриптивной модели *L*(*P*) характеризуется тем, что при формализации различных аспектов такого представления используемые ДЭП могут быть как межаспектными (общими для нескольких аспектов), так и внутриаспектными (используемыми при описании конкретного аспекта). Учет межаспектных ДЭП обеспечивает интеграцию частных модельных представлений $L_\eta(P)$ в единую дескриптивную модель *L*(*P*).

Заключение

Предлагаемая дескриптивная модель *L(P)* обеспечивают целостное многоаспектное представление процесса оперативного восстановления изделий СТК, в котором осуществляется согласование формализованного представления этого процесса с его понятийным представлением, основанным на использовании средств естественного языка. Использование предлагаемой дескриптивной модели предоставляет возможность личному составу дежурной смены определять требовании к необходимой оперативной информации в запросах на естественно-подобном языке с использованием предметных понятий и терминов. Формализация, заложенная в предлагаемой дескриптивной модели, обеспечивает интерпретацию таких запросов и формирование необходимой оперативной информации, определяемой информационным ресурсом в виде существующей базы данных для процесса оперативного восстановления.

Рассматриваемое использование дескриптивной модели приводит к совершенствованию существующих

средств автоматизации рассматриваемого процесса в части информационной поддержки. Это способствует уменьшению времени оперативного восстановления изделий СТК за счет сокращения времени формирования оперативной информации в деятельности личного состава дежурной смены.

Литература

1. *Шеер А.-В.* Моделирование бизнес-процессов: пер с англ. 2-е изд. М.: Весть-МетаТехнология, 2000. 222 с.

2. *Анисимов О.В., Курчидис В.А.* Методы информационной поддержки обслуживающего персонала при восстановлении радиоэлектронной аппаратуры // Материалы всероссийской научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения» (Москва, 14 мая 2014). Москва, 2014. С. 33–45.

3. *Марка Д.А., МакГоуэн К.Л.* Методология структурного анализа и проектирования SADT: пер. с англ. М.: Мета Технология, 1993. 239 с.

4. *Страхов О.А., Страхов А.Ф., Криволапов В.Л., Пономарев В.И.* Состав баз данных и баз знаний, используемых в задачах обеспечения эксплуатации группировок ВВТ ПВО // Вопросы радиоэлектроники. 2018. № 6. С. 39–43.

5. *Киммел П.* UML. Основы визуального анализа и проектирования: раскрытие тайн; UML. Универсальный язык программирования: самоучитель: пер. с англ. М.: NT Press, 2008. 264 с.

6. *Поспелов Д.А.* Логико — лингвистические модели в системах управления. М.: Энергоиздат, 1981. 232 с.

7. *Пономарев В.И., Страхов А.Ф.* Пути повышения оперативности разрешения нештатных ситуаций на образцах вооружения и военной техники воздушно-космической обороны российской федерации // Вестник воздушно-космической обороны. 2015. № 4(8). С. 108–115.

8. *Пономарев В.И., Страхов А.Ф.* Особенности управления жизненным циклом сложных технических систем в современных условиях // Вестник воздушно-космической обороны. 2016. № 1(9). С. 98–106.

9. *Калик Н.А., Страхов А.Ф.* Концепция обеспечения требуемого уровня готовности территориальных группировок ВТ ПВО с учетом нештатных ситуаций // Вестник Концерна ПВО «Алмаз — Антей». 2011. № 3(5).

10. РД IDEF 0–2000. Методология функционального моделирования IDEF0. М.: Госстандарт России, 2000, 75 с.

11. *Репин В.В., Елифеев В.Г.* Процессный подход к управлению. Моделирование бизнес процессов. М.: Стандарты и качество, 2004. 408 с.

12. *Маклаков С.В.* Моделирование бизнес-процессов BPWin. М.: ДиалогМИФИ, 2002. 209 с.

13. *Фаулер М.* UML. Основы. Краткое руководство по стандартному языку объектного моделирования: пер. с англ. 3-е издание. СПб.: Символ-Плюс, 2004. 192 с.

14. *Яковлев С.А., Швецов А.Н.* Архитектура баз знаний в распределенных интеллектуальных информационных системах // Материалы межд. науч.-техн. конф. «Информатизация процессов формирования открытых систем на основе СУБД, САПР, АСНИ и искусственного интеллекта» (26–28 июня 2001 г.). Вологда: Изд-во ВоГТУ, 2001. С. 124–128.

15. *Рассел С., Норвиг П.* Искусственный интеллект: современный подход: пер с англ. М.: Вильямс, 2006. 1408 с.

16. *Baader F., Calvanese D., McGuinness D. L., Nardi D., Patel-Schneider P. F.* The Description Logic Handbook: Theory, Implementation, and Applications. Cambridge University Press, 2003.

FORMALIZED REPRESENTATION OF THE TECHNICAL COMPLEXES OPERATIVE RESTORATION PROCESS AS A DESCRIPTIVE MODEL

OLEG V. ANISIMOV,
Yaroslavl, Russia, qwaker@inbox.ru

VIKTOR A. KURCHIDIS,
Yaroslavl, Russia, idahmer2@yandex.ru

VADIM A. KOROBKO,
Yaroslavl, Russia, vadym.korobko@yandex.ru

KEYWORDS: operative restoration; information support; descriptive model; descriptive elements of process representation; automation.

ABSTRACT

The operative restoration process of weapons and military equipment from the point of view of its model representation is considered. It is intended for the automation of the duty personnel activities of the situational management of repair and maintenance of air defense groups center. It is proposed to reduce the time of operational information formation due to the transition to a formal representation of this process.The limitations of the existing model representations of the considered process used in the automation tools of this center are presented. The existing limitations lead to the multiple simultaneous interpretation of data and subject concepts of the operative restoration process in the activities of the duty shift of the situation management center, which negatively affects the technical complexes operative restoration time. An approach to the formalization of the model representation of such a process is proposed, which extends the capabilities of existing models and allows to formalize the semantic links between the elements of the operative restoration process in terms of natural language. The proposed formalized representation of the process belongs to the class of descriptive models and focuses on the combination of a logical description of this process with its description in natural language. This reduces the unproductive time spent on the formation of operational information. Using the proposed descriptive models in the automation of the situation management centre aimed at reducing of weapons and military equipment of air defense group operative restoration time at the expense of reduction of operational information formation time in the activities of the duty personnel.

REFERENCES

1. Scheer A.-V. *ARIS – Business Process Modeling*. Springer-Verlag Berlin, Heidelberg, 1999. 220 p.
2. Anisimov O.V., Kurchidis V.A. Metody informacionnoj podderzhki obsluzhivayuschego personala pri vosstanovlenii radio`elektronnoj apparatury [Methods of information support of the service personnel at restoration of radio-electronic equipment]. *Materialy vserossijskoj nauchnoj konferencii "Sovremennye tendencii razvitiya teorii i praktiki upravleniya v sistemah special'nogo naznacheniya"* [Proc. of the All-Russia scientific conference "Current trends of development of the theory and practice of management in systems of a special purpose", Moscow, 14 may 2014]. Moscow, 2014. Pp. 33–45. (In Russian)
2. Marca D.A., McGowan C.L. *SADT: Structure Analysis and Design Techniques*. New York: McGraw Hill Publ., 1988. 392 p.
3. Strakhov O.A., Strakhov A.F., Krivolapov V.L., Ponomarev V.I. Composition of data and knowledge bases used for tasks aimed at ensuring ad wme groups operation. *Voprosy radioèlektroniki* [Radio electronics]. 2018. No. 6. Pp. 39–43. (In Russian)
4. Kimmel P. UML. Demystified. McGraw-Hill Osborne, 2005. 235 p.
5. Pospelov D.A. *Logiko – lingvisticheskie modeli v sistemah upravleniya* [Logic – linguistic models in control systems]. Moscow: Energoizdat, 1981. 232 p. (In Russian)
6. Ponomarev V.I., Strakhov A.F. Enhancing procedures of resolution responsiveness of contingency situations on arms and military equipment samples of the russian federation aerospace defense force. *Vestnik vozdušno-kosmičeskoj oborony* [Aerospace Defense Herald]. 2015 No. 4 (8). Pp. 108–115. (In Russian)
7. Ponomarev V.I., Strakhov A.F. Particularities of complex technical systems life cycle management in modern conditions. *Vestnik vozdušno-kosmičeskoj oborony* [Aerospace Defense Herald]. 2016. No. 1(9). Pp. 98–106. (In Russian)
8. Kalik N.A., Strakhov A.F. Koncepciya obespecheniya trebuemogo urovnya gotovnosti territorial'nyh gruppirovok VT PVO s uchetom neshtatnyh situacij [The concept of providing demanded level of readiness of the air defenses W territorial groups taking into account emergency situations]. *Bulletin of Concern PVO Almaz-Antey*. 2011. No. 3(5). (In Russian)
9. RD IDEF 0–2000. Metodologiya funkcional'nogo modelirovaniya IDEF0 [Metodologiya funkcional'nogo modelirovaniya IDEF0]. Moscow: Gosstandart Rossii, 2000, 75 p. (In Russian)
10. Repin V.V., Elifeev V.G. *Processnyj podhod k upravleniyu. Modelirovanie biznes processov* [Process approach to management. Modeling business of processes]. Moscow: Standarty i kachestvo, 2004. 408 p. (In Russian)

11. Maklakov S.V. *Modelirovanie biznes-processov BPWin* [Modeling of business processes of BPWin]. Moscow: DialogMIFI, 2002. 209 p. (In Russian)
12. Fowler M. *UML Distilled A Brief Guide to the Standard Object Modeling Language*. 3rd edition. Addison Wesley, 2003. 192 p.
13. Yakovlev S.A., Shvecov A.N. Arhitektura baz znanij v raspredelennyh intellektual'nyh informacionnyh sistemah [Architecture of knowledge bases in the distributed intellectual information systems]. *Materialy mezhdunarodnoj nauchno-tehnicheskoj konferencii "Informatizaciya processov formirovaniya otkrytyh sistem na osnove SUBD, SAPR, ASNI i iskusstvennogo intellekta"* [Proc. of the international scientific and technical conference "Information of processes of formation of open systems on the basis of DBMS, SAPR, ASNI and artificial intelligence", Vologda, June 26–28, 2001]. Vologda, 2001. Pp. 124–128. (In Russian)
14. Russell S.J., Norvig P. *Artificial Intelligence: A Modern Approach*. 2nd. ed. New Jersey: Prentice Hall, Upper Saddle River, 2003. 1132 p.
16. Baader F., Calvanese D., McGuinness D. L., Nardi D., Patel-Schneider P. F. *The Description Logic Handbook: Theory, Implementation, and Applications*. Cambridge University Press, 2003.

INFORMATION ABOUT AUTHORS:
Anisimov O.V., PhD, Docent, Professor of the Yaroslavl Higher Military College Of Anti-Air Defense.
Kurchidis V.A., PhD, Professor, Professor of the Yaroslavl Higher Military College Of Anti-Air Defense.
Korobko V.A., Postgraduate of the Yaroslavl Higher Military College Of Anti-Air Defense.

For citation: Anisimov O.V., Kurchidis V.A., Korobko V.A. Formalized representation of the technical complexes operative restoration process as a descriptive model. *H&ES Research*. 2019. Vol. 11. No. 4. Pp. 14–21. doi: 10.24411/2409-5419-2018-10283 (In Russian)

doi: 10.24411/2409-5419-2018-10284

МОДЕЛЬ ЗАЩИТЫ ОТ ЭКСПЛОЙТОВ И РУТКИТОВ С ПОСЛЕДУЮЩИМ АНАЛИЗОМ И ОЦЕНКОЙ ИНЦИДЕНТОВ

САХАРОВ
Дмитрий Владимирович[1]

КОВЦУР
Максим Михайлович[2]

БАХТИН
Дмитрий Витальевич[3]

АННОТАЦИЯ

В современных распределенных информационных системах преобладают различного вида и характера угрозы связанные с несанкционированным доступом и утечкой данных. Имеются угрозы, которые направленны на нанесение вреда личным данным пользователя посредством их повреждения или копирования для своей личной выгоды в целях использованиях непосредственно против самого пользователя. В качестве примера следует упомянуть такие сетевые угрозы (атаки) типа эксплоит и руткит. В данной работе рассмотрены о модели защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов. Обратная разработка подразумевается как «исследование некоторого устройства или программы, а также документации на них с целью понять принцип его работы и, чаще всего, воспроизвести устройство, программу или иной объект с аналогичными функциями, но без копирования как такового». Реверс программного обеспечения применяется для анализа и взлома, а также для исследования работы вредоносных программ, с целью их дальнейшего обезвреживания. Тестирование вредоносного кода – это целая наука в области предоставления информационной безопасности. Такими вещами занимаются и специальные антивирусные лаборатории, которые в свою очередь выпускают эти самые продукты для предоставления защиты, и узконаправленные группы специалистов, а также сами вирусописатели. Анализ кода требует нестандартного и креативного подхода, не существует универсальной методики для успешного взлома. Однако, общие методики анализа, которым следует придерживаться, уже довольно длительное время остаются неизмененными. Иными словами, реверс – исследование и воссоздание алгоритмов деятельности программы без исходных кодов.

Сведения об авторах:

[1]к.т.н., доцент Санкт-Петербургского государственного университет телекоммуникаций имени профессора М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия

[2]к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, maxkovzur@mail.ru

[3]студент магистратуры Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, Drivan289@gmail.com

КЛЮЧЕВЫЕ СЛОВА: Exploit; руткит; эксплойт; несанкционированный доступ; распределенные информационные системы; информационная безопасность.

Для цитирования: *Сахаров Д.В., Ковцур М.М., Бахтин Д.В.* Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22-9. doi: 10.24411/2409-5419-2018-10284

В настоящее время известно, что большинство современных эксплойтов реализуется через определенные процессы внутри операционной системы. Для того чтобы разобраться с ними, а также с таким явлением как руткиты следует разобраться с обратным инжинирингом.

Обратный инжиниринг предполагается как «исследование некоторого устройства или программы, а также документации на них с целью понять принцип его работы и, чаще всего, воспроизвести устройство, программу или иной объект с аналогичными функциями, но без копирования как такового». Реверс программного обеспечения применяется для анализа и взлома, а также для исследования работы вредоносных программ, с целью их дальнейшего обезвреживания.

Тестирование вредоносного кода — это целая наука в области предоставления информационной безопасности [1]. Такими вещами занимаются и специальные антивирусные лаборатории, которые в свою очередь выпускают эти самые продукты для предоставления защиты, и узконаправленные группы специалистов, а также сами вирусописатели. Анализ кода требует нестандартного и креативного подхода, не существует универсальной методики для успешного взлома. Однако, общие методики анализа, которым следует придерживаться, уже довольно длительное время остаются неизмененными [2]. Иными словами, реверс — исследование и воссоздание алгоритмов деятельности программы без исходных кодов. По сравнению с анализом вредоносных программ тут возникает несколько нюансов:

Во-первых, обратный инжиниринг программного обеспечения чаще всего запрещено использовать по правилам лицензионного соглашения. Вот, например, как выглядит лицензионное соглашение для *Kaspersky Rescue Disk* 10: «Запрещается декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на программном обеспечении, целиком или частично за исключением случаев, предусмотренных применимым законодательством». Анализ же вирусов таких ограничений не содержит, более того, это «дело благородное».

Во-вторых, обратный инжиниринг, чаще всего, используется для коммерческого программного обеспечения, делающего из «пробного» или незарегистрированного продукта программного обеспечения вполне рабочую. Другими словами, это распространение нелегальных копий продукта программного обеспечения. Подобные операции нарушают большое число статей об авторском и интеллектуальном праве, патентном законодательстве, международном соглашении и так далее.

Нередко встречается, что при анализе вредоносного программного обеспечения в распоряжении исследователя есть только исполняемый файл или библиотека, скомпилированная в двоичном виде. Для того чтобы понять, как бинарный код работает, необходимо использовать специальные подходы и методы. Известно два главных метода к анализу такого рода программ: статический и динамический. При статическом анализе программы изучают, не запуская их на исполнение. Динамический же анализ включает в себя запуск программ и манипуляции с ними в оперативной памяти. Таким образом эти два подхода возможно поделить на базовый и продвинутый анализ. Базовый статический анализ заключается в исследовании исполняемого файла без просмотра машинных инструкций. В свою очередь базовый динамический анализ напрямую связан с запуском программы и наблюдением за ее поведением в системе. Продвинутый статический анализ представляет из себя загрузку исполняемого файла в дизассемблер без выполнения кода в оперативной памяти, а также возможность просмотра ассемблерных инструкций с возможностью узнать, что делает данный код программы в системе. Продвинутый динамический анализ применяет отладчик с целью узнать внутреннее состояние выполняемого кода в оперативной памяти [3].

Дизассемблер *IDA Pro*. Это интерактивный дизассемблер, который обширно применяется для обратного инжиниринга. Он различается своей уникальной гибкостью, наличием интегрированного командного языка, также поддержка большого количества различных форматов исполняемых файлов для множества процессоров и операционных систем. Такой функционал дает возможность создавать различные блок-схемы, менять названия меток, изучать локальные процедуры в стеке и многое другое.

На примере работы с известным интерактивным дизассемблером *Ida Pro* будут рассмотрены некоторые доступные (для ознакомительных и изучающих мер) *exploit* программы [4].

В ходе работы с первым кандидатом (рис. 1) стоить обратить внимание на отличающуюся библиотеку в разделе «*Imports*», а также его описанию «*AdjustTokenPrivileges*», что в дословном переводе может означать настройку прав доступа или же привилегий (рис. 2). Исходя из таких данных можно сделать вывод, что злоумышленник пытается изменить или подкорректировать права доступа пользователя в операционной системе, что может повлечь за собой необратимые последствия.

Далее известной нам проблеме находим ее в коде ассемблера и подтвердив свои опасения следует предпринять необходимые средства защиты для противодействия от *exploit*.

В качестве упреждающих мер следует постараться вовремя засечь вторжение в операционную систему. Из самых простых средств защиты стоит отметить обычный, классический мониторинг системных логов, скачанных программ и всего трафика целиком.

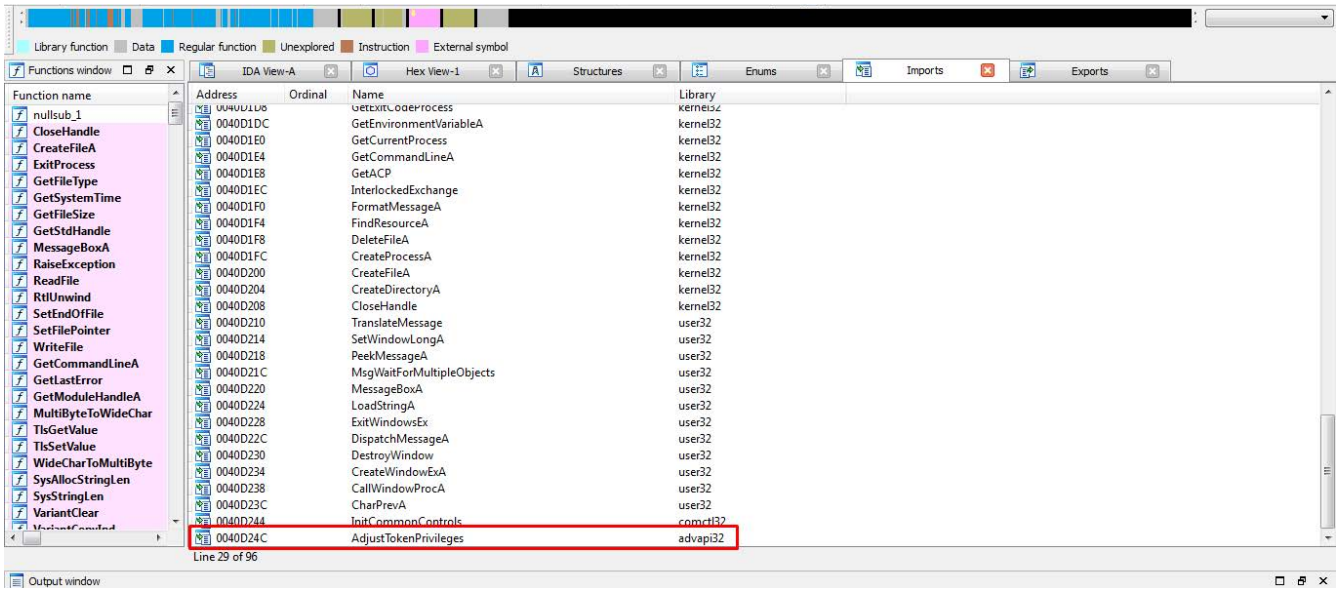


Рис. 1. Пример подозрительного адреса в программном обеспечении

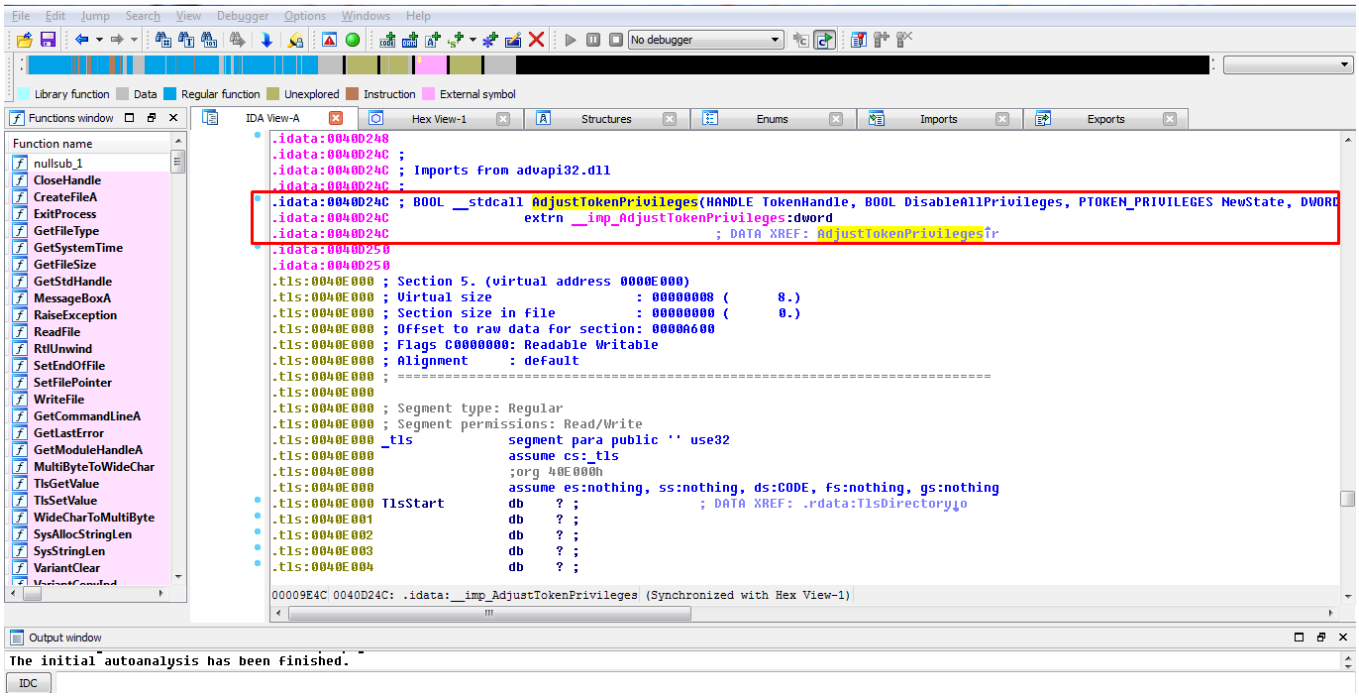


Рис. 2. Подозрительная сигнатура в коде ассемблера

Большинство злоумышленников заранее предполагают о том, что их деятельность будет обнаружена, поэтому они постоянно стараются думать наперед и отсрочить время их обнаружения и дальнейшего устранения из системы. По этой причине чаще всего их задачей является получить максимум информации за время доступа к системе. Естественно, они будут пытаться скрыть свое присутствие руткитами и другими подобными методами.

Если рассматривать *Windows* 10 в ней имеется уже встроенная система обнаружения и защиты от *exploit* программ.

Из наиболее важных и известных мер имеются такие как:

1. Предоставление защиты потока управления
2. Предотвращение выполнения данных системы
3. Принудительное случайное распределение для образов

4. Случайное распределение выделения памяти системы
5. Проверка цепочек исключений
6. Проверка целостности “кучи”
7. Защита от произвольного кода
8. Блокировка образов низкой целостности
9. Блокировка удаленных образов
10. Блокировка ненадежных шрифтов
11. Защита целостности кода
12. Отключение точек расширения
13. Отключение вызовов системы *Win32k*
14. Не разрешать дочерние процессы
15. Фильтрация адресов экспорта (*EAF*)
16. Фильтрация адресов импорта (*IAF*)
17. Имитация выполнения (*SimExec)*
18. Проверка вызовов *API* (*CallerCheck*)
19. Проверка использования дескриптора
20. Проверка целостности зависимостей образа
21. Проверка целостности стека (*StackPivot*)

Также всегда можно использовать командную строку *PowerShell* для работы с необходимыми мерами против сетевых атак. В свободном доступе в интернете есть команды, которые помогут более детально рассмотреть все защитные меры выбранных процессов.

Из простых средств защиты против любых утечек информации следует упомянуть своевременный “бекап” всей важной информации на внешние носители памяти или же хранить важные данные в облачных хранилищах (первое наиболее безопасно, но зависит непосредственно от самого облака).

Любое антивирусное программное обеспечение также не стоит обходить стороной. В некоторых из них есть отдельные более углубленные настройки защиты мер против *exploit* программ. Например, *Kaspersky lab* благодаря своему обширному многообразию различных контрмер [5].

Поэтому для формализации понятий события и инцидента безопасности первоначально требуется создать модель (рис. 3), описывающую предметную область с точки зрения взаимодействующих устройств. В данной статье представлена математическая модель взаимодействия устройств, на основе которой формализовано понятие события контроля учета рабочего времени, а также доказана достаточность

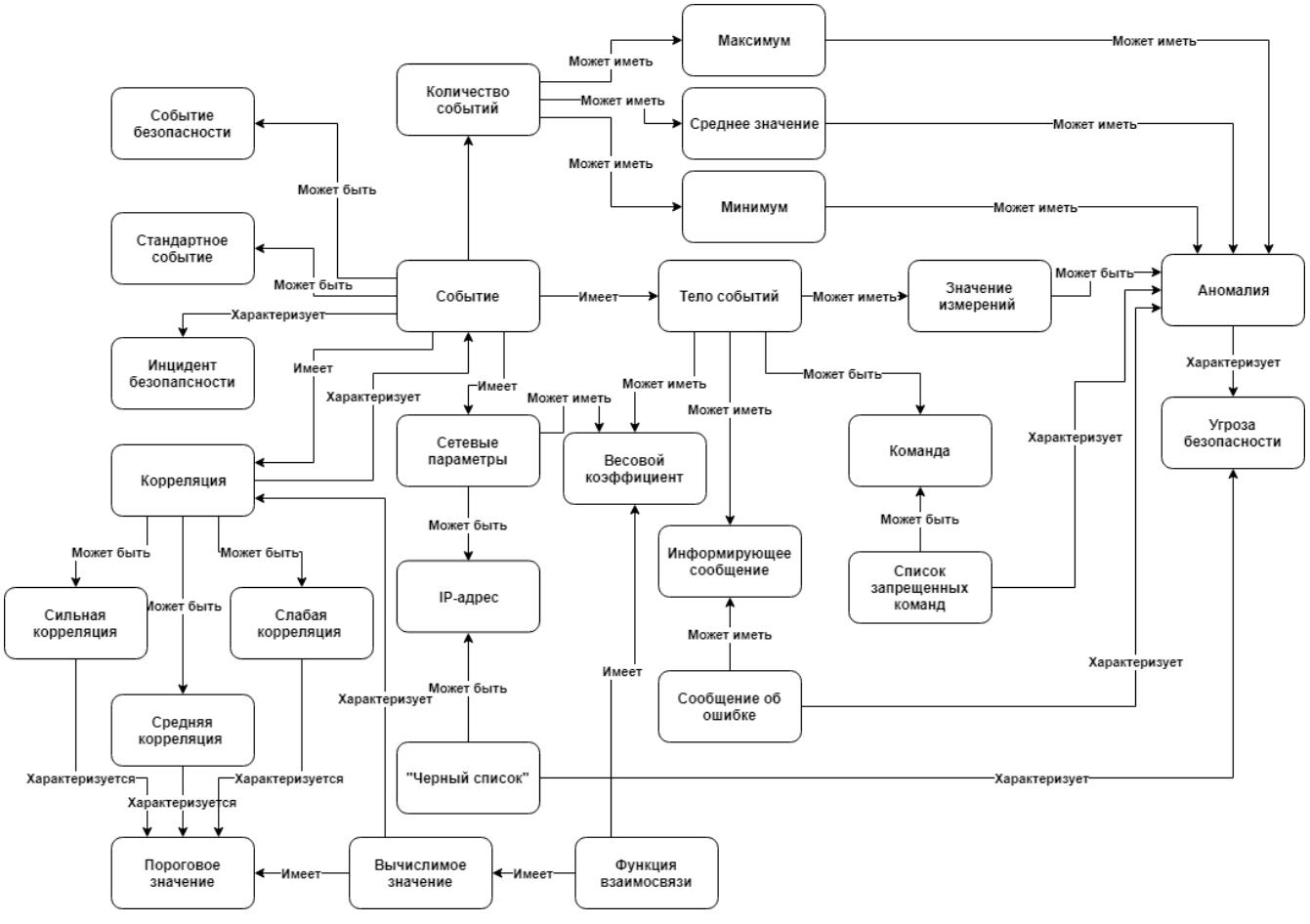


Рис. 3. Модель защиты от эксплойтов и руткитов

анализа синхронизации разных механизмов работы систем защиты информации для осуществления данного контроля.

Модель, учитывающая данные уровни, позволит агрегировать разные состояния больших массивов данных для систем контроля учета рабочего времени сотрудников [6]. В соответствии с синхронизацией в распределенных информационных системах, для сокращения размерности пространства сообщений, с целью последующей его трансформации в пространство событий, требуется выполнить этот этап агрегации. Представлена (см. рис. 4) общая схема процесса предварительной обработки данных от устройств распределенных информационных системах, состоящая из следующих этапов:

1) агрегация сообщений в соответствии с сетевыми параметрами;

2) нормализация сообщений;

3) агрегация сообщений в соответствии с типом устройства;

4) формирование событий из сообщений.

Соответственно получается, что первичная агрегация в памяти может производиться с разной интенсивностью в зависимости от устройства. Также имеет значение возможная потеря данных, так как до занесения агрегированного значения в хранилище обработка происходит в оперативной памяти и в случае сбоя поступившие сведения могут быть потеряны.

Подобная модель может быть применима к современным средам систем электронного документооборота. К примеру, представление того, что информационная система, которая поддерживает документооборот компании, считается инструментом улучшения, однако никак не его синонимом, приходит в компанию не сразу. Подобного рода введения чаще всего сопряжены с значительными нововведениями в процессах документооборота. Данные процессы при введении подвергаются обратному инжинирингу, то есть полной перестройке, для того чтобы информационная система в совокупности с данными нововведениями смогла преподнести компании, в которой произошло введение, максимальную отдачу. Непосредственно сам процесс введения данной информационной системы электронного документооборота, заключает в себя нескольких этапов, методологически стандартизованных для различных компаний. Данные этапы применения модели могут помочь включить эту систему электронного документооборота и для множества ситуаций выглядят идентично (рис. 5):

1. Исследование системы документооборота;

2. Создание технического задания на автоматизацию документооборота;

3. Адаптирование системы электронного документооборота для требований технического задания;

4. Внедрение системы в опытную эксплуатацию, а также подготовка (обучение) пользователей;

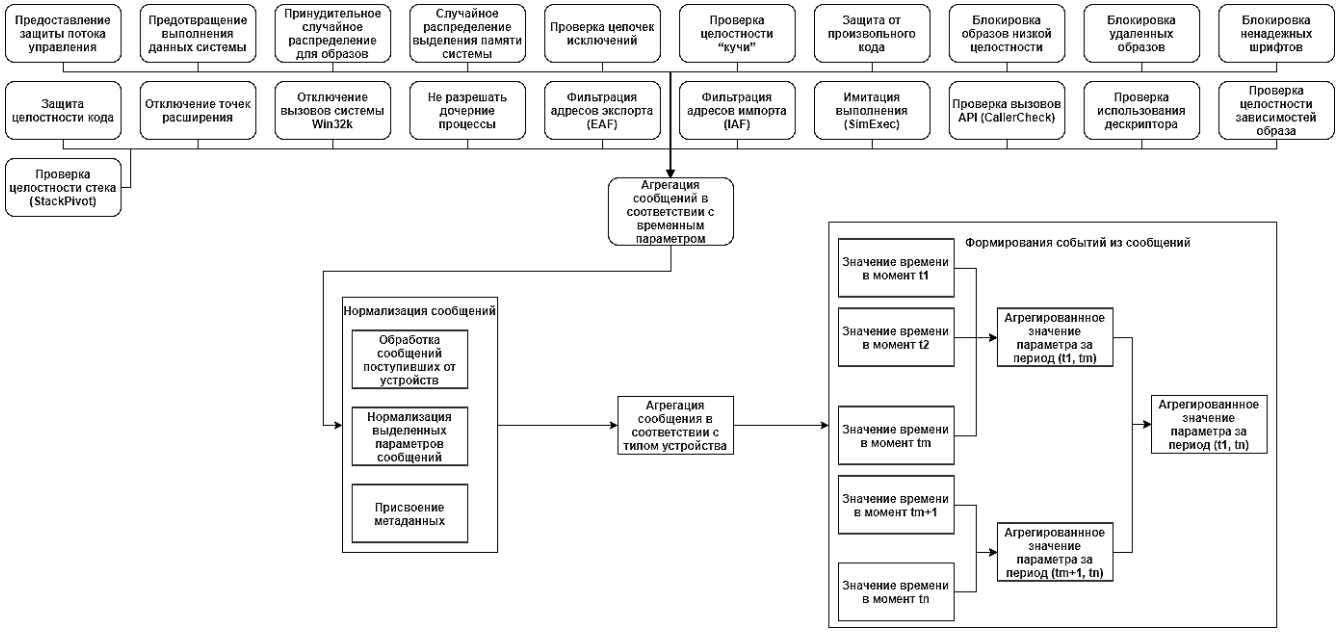


Рис. 4. Взаимосвязь разработанных математических методов агрегации больших массивов данных. Схема агрегации сообщений в методике по времени

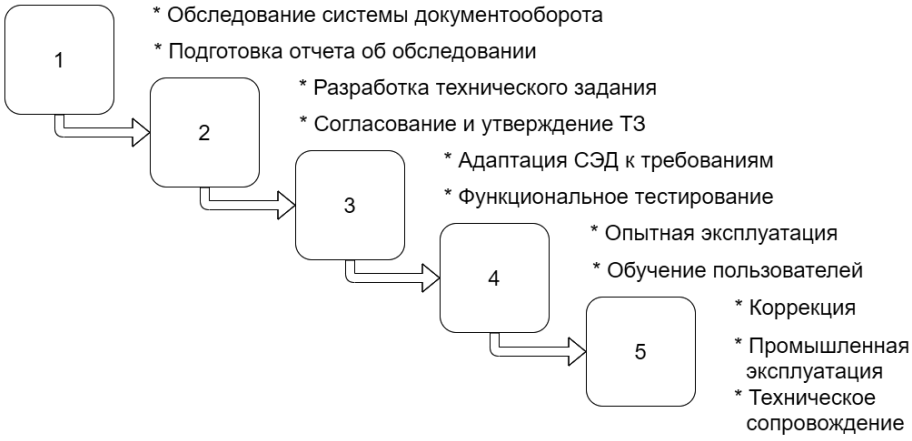


Рис. 5. Этапы внедрения системы электронного документооборота

5. Испытания для приема и ввода данной системы электронного документооборота в промышленную эксплуатацию.

Несомненно, что одной покупки программы в данном случае на хватит.

Задачей первого этапа будет считаться проверка и документирование имеющейся в компании системы документооборота (бумажной).

Однако вопреки тому, что имеющаяся система способна не удовлетворять, она включается в себя большое количество аспектов, которые обязаны быть сохранены при введении автоматизированной системы (требования к формам документов, отчетности, структуре прохождения согласования и пр.).

В последствии одобрения технического задания разработчик организации, исполняющий введение, приступают налаживать систему электронного документооборота в согласовании с условиями технического задания. В результате уже отлаженная система проходит функциональную проверку и запускается в опытную эксплуатацию [7].

На данном этапе в организации обязательно будет происходить массовая подготовка (обучение) к использованию новой системы, но допустимо и обнаружение тех или иных нарушений в работе этой системы, которые на данном этапе чаще всего мгновенно исправляются разработчиками.

Некоторые элементы, произведенные, приводят к изменению соотношений нулей и единиц (операции по сбору данных производились с 32 локальных компьютеров в информационных системах около 100 раз на каждом, потому данная таблица отражает сведения с одного компьютера).

Проведенный анализ показывает, что действия методики защищенного контроля учета по выработанным способам не всегда срабатывают, однако их точный анализ дает основание для формирования мониторинга по дальнейшему статистическому анализу заявленных результатов.

И последовательности событий по мониторингу следующие [8]: Этап атаки 1 (хост web-server) -> Этап атаки 2 (хост DB server)-> Этап атаки 3 (хост proxy server) -> Этап атаки 4 (хост Application server) -> Этап атаки 5 (хост Mail server). По исходящей зависимости стало возможным определение конечных потерь до и после внедрения методики защищенного контроля учета. Для проверки действия методики были разделены все 5 этапов, которые одновременно запускались в информационной системе. Следует отметить, что методика, по результатам тестов стала дополнением метода мониторинга, сместив начальные позиции потерь в представленной модели обработки данных. Результаты экспериментов представлены в табл. 1.

Входными данными модели являются: N — модель обработки данных; S — методика сбора данных; A — методика обнаружения вторжений; M — модель атакующего; E — модель событий. Необходимыми для оценки являются как минимум модели N и S. Остальные модели являются дополнительными и позволяют получить более точную оценку. Модель E отвечает за оценку защищенности в динамическом режиме [9]. Входными данными методики выбора защитных мер являются: комплекс показателей защищенности (результат работы методики оценки защищенности) и модели R защитных мер. Пусть R_a — риск успешной реализации. R_a является результатом работы функции определения риска атаки. Обозначим как C — множество средств защиты и защитных мер, рекомендуемых системой оценки защищенности и выбора защитных мер для атаки. Тогда результат работы функции $R_a(C)$ — риск успешной реализации атаки а в случае реализации защитных мер C. Целевой функцией методики оценки за-

Таблица 1

Результаты экспериментов по определению потерь и временных
в случае реализации методики контроля учета в ИС

Последовательность атаки	**Потери после, бит/с**	**Потери до, бит/с**	**Время на обнаружение, сек**
Результаты экспериментов с 50% мощностью атаки			
Этап 1	0,2	5,4	8
Этап 2	0,6	5,1	7
Этап 3	0,8	7,1	14
Этап 4	0,4	5,9	10
Этап 5	0,4	2,2	5
Процент ошибок первого рода		**Процент ошибок второго рода**	
Потери после, бит/с	**Потери до, бит/с**	**Потери после, бит/с**	**Потери до, бит/с**
0,8	0,47	0,6	0,38
0,38	0,27	0,09	0,1
1,85	1,88	2,96	1,75
1,54	1,3	0,8	1,05
Результаты экспериментов с 80% мощностью атаки			
Этап 1	0,2	5,4	8
Этап 2	0,6	5,1	7
Этап 3	0,8	7,1	14
Этап 4	0,4	5,9	10
Этап 5	0,4	2,2	9
Процент ошибок первого рода		**Процент ошибок второго рода**	
Потери после, бит/с	**Потери до, бит/с**	**Потери после, бит/с**	**Потери до, бит/с**
0,33	0,24	0,42	0,28
0,25	0,16	0,07	0,09
0,78	0,85	2,4	1,44
1,71	1,7	1,33	1,07
Результаты экспериментов с 100 % мощностью атаки			
Этап 1	0,2	5,4	8
Этап 2	0,6	5,1	7
Этап 3	0,8	7,1	14
Этап 4	0,4	5,9	8
Этап 5	0.4	2,2	7
Процент ошибок первого рода		**Процент ошибок второго рода**	
Потери после, бит/с	**Потери до, бит/с**	**Потери после, бит/с**	**Потери до, бит/с**
0,24	0,42	0,28	0,18
0,16	0,07	0,09	0,11
0,87	2,4	1,47	0,32
1,8	1,32	1,07	0,25

щищенности и выбора контрмер является снижение риска в случае атак на информационные системы [10].

Данная модель защиты от эксплойтов и руткитов позволила выявить серьезную устойчивость по отношению к ошибкам I и II рода.

В целом по табл. 1 разработанная модель демонстрирует положительную динамику сокращения деструктивных воздействий на информационные системы. Уровень ошибок I рода в пределах от 0,5% до 1,5%, вероятность ошибок II рода от 1% до 2%.

Литература

1. *Буйневич М.В., Израилов К.Е.* Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура // Информационные технологии и коммуникации. 2016. Т. 4. № 1. С. 115–130.

2. *Израилов К.Е.* Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура // Информационные технологии и коммуникации. 2016. Т. 4. № 2. С. 86–104.

3. *Штеренберг С.И.* Методика применения языка ассемблер для стеговложения информации в иссполняемые файлы // T-comm: Телекоммуникации и транспорт. 2016. Т. 10. № 6. С. 42–47.

4. *Штеренберг С.И., Андрианов В.И.* Исследование методики адаптивных атак на основе скрытого вложение в исполняемые файлы // Сборник статей Международной научно-технической конференции «Наука, техника, инновации» (Брянск, 25–27 марта 2014 г.). Брянск: Надежные машины, 2014. С. 287–294.

5. *Пестов И.Е., Сахаров Д.В., Сергеева И.Ю., Чернбородов И.С.* Выявление угроз безопасности информационных систем // Сборник научных статей VI Международной научно-технической и научно-методиче-ской конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, 01–02 марта 2017 г.). СПб.: Изд-во Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. Т. 2. С. 525–527.

6. Что такое эксплойты и почему их все так боятся? // Лабо ратория Касперского. URL: https://www.kaspersky.ru/blog/exploits-problem-explanation/8459/ (дата обращения 15.10/2019).

7. *Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е.* Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.

8. *Андрианов В.И., Виткова Л.А., Сахаров Д.В.* Исследование алгоритма защиты общедоступных персональных данных в информационных системах // Сборник научных статей V международной научно-технической и научно-методической конференции «Акутальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, 10–11 марта 2016 г.). СПб.: Изд-во Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. Т. 1. С. 227–231.

9. *Андрианов В.И., Крылов А.И.* Решение задачи при классификации уязвимостей автоматизированных систем // Журнал научных публикаций аспирантов и докторантов. 2010. № 9(51). С. 99–101.

10. *Андрианов В.И., Андронов А.В.* Интеллектуальные средства обеспечения информационной безопасности автоматизированных систем в условиях неопределенности // Журнал научных публикаций аспирантов и докторантов. 2010. № 8(50). С. 120–121.

MODEL OF PROTECTION AGAINST EXPLOITS AND ROOTKITS WITH THE FOLLOWING ANALYSIS AND ASSESSMENT OF INCIDENTS

DMITRY V. SAKHAROV,
St. Petersburg, Russia

MAXIM M. KOVTSUR,
St. Petersburg, Russia, maxkovzur@mail.ru

DMITRY V. BAKHTIN,
St. Petersburg, Russia, Drivan289@gmail.com

KEYWORDS: exploit; rootkit; unauthorized access; distributed information systems; information security.

ABSTRACT

In modern distributed information systems, various types and nature of threats are associated with unauthorized access and data leakage. There are threats that are intended to harm the user's personal data by damaging or copying them for their own personal benefit in order to use directly against the user. As an example, mention should be made of such network threats (attacks) such as exploits and rootkits. This work deals with the model of protection against exploits and rootkits with subsequent analysis and evaluation of incidents. Reverse engineering is meant as "the study of some device or program, as well as documentation on them in order to understand its principle of operation and, most often, reproduce a device, program or other object with similar functions, but without copying as such". The reverse of the software is used for analysis and hacking, as well as for investigating the operation of malicious programs, with a view to their further neutralization. Malware testing is a science in the field of information security. Special antivirus laboratories, which in turn release these same products to provide protection, and narrowly focused groups of specialists, as well as virus writers themselves, are involved in such things. Code analysis requires a non-standard and creative approach; there is no universal technique for successful hacking. However, the general methods of analysis that should be followed for a rather long time remain unchanged. In other words, the reverse is the study and reconstruction of the algorithms of the program without source codes.

REFERENCES

1. Buinevich M.V., Izrailov K.E. Utility for Vulnerability Search in a Software of Telecommunication Devices by Method Algoritmization of Machine Code. Part 1. Functional Architecture. *Informatsionnye tekhnologii i kommunikatsii* [Information technology and communications]. 2016. Vol. 4. No. 1. Pp. 115–130. (In Russian)

2. Izrailov K.E. Utility for vulnerability search in software of telecommunication devices by method algorithmization of machine code. Part 2. Information architecture. *Informatsionnye tekhnologii i kommunikatsii* [Information technology and communications]. 2016. Vol. 4. No. 2. Pp. 86–104. (In Russian)

3. Shterenberg S.I. The method of application assembler programming language for concealed attachment information in executables. *T-Comm*. 2016. Vol. 10. No.6. Pp. 42–47. (In Russian)

4. Shterenberg S.I., Andrianov V.I. Adaptive research methods based attacks hidden attachments in the executive files. *Cbornik statey Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii "Nauka, tekhnika, innovatsii"* [Proc. of articles of the International scientific and technical conference" Science, technology, innovation", Bryansk, March 25–27, 2014]. Bryansk: Reliable machines, 2014. Pp. 287–294. (In Russian)

5. Pestov I.E., Sakharov D.V., Sergeeva I. Yu., Chernborodov I.S. The Detection of the Security Threats to Information Systems. *Sbornik nauchnykh statey VI mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii "Akutal'nye problemy infotelekommunikatsiy v nauke i obrazovanii"* [Proc. of scientific articles of the VI international scientific-technical and scientific-methodical conference "Actual problems of infotelecommunications in science and education", St. Petersburg, March 01–02, 2017)]. St. Petersburg, 2017. Vol. 2. Pp. 525–527. (In Russian)

6. Chto takoe eksployty i pochemu ikh vse tak boyatsya? [What are exploits and why are they all so afraid of them?] // Kaspersky daily Rezhim dostupa: https://www.kaspersky.ru/blog/exploits-problem-explanation/8459/, svobodnyy. (In Russian)

7. Krasov A.V., Shterenberg S.I., Fakhrutdinov R.M., Ryzhakov D.V., Pestov I.E. Analysis of the information security of the enterprise based on data collection of users from open resources and mon-

itoring of information resources with the use of machine learning. *T-Comm*. Vol. 12. No. 10. Pp. 36–40. (In Russian)
8. Andrianov V.I., Vitkova L.A., Sakharov D.V. Research of Algorithm Protection Public Personal Data in Information Systems. *Sbornik nauchnykh statey V mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii "Akutal'nye problemy infotelekommunikatsiy v nauke i obrazovanii"* [Proc. of scientific articles of the V international scientific-technical and scientific-methodical conference "Actual problems of infotelecommunications in science and education", St. Petersburg, March 10–11, 2016)]. St. Petersburg, 2016. Vol. 1. Pp. 227–231. (In Russian)
9. Andrianov V.I., Krylov A.I. Reshenie zadachi pri klassifikatsii uyazvimostey avtomatizirovannykh sistem [The solution of the problem in the classification of vulnerabilities in automated systems]. *Zhurnal nauchnykh publikatsiy aspirantov i doktorantov* [Journal of scientific publications of postgraduates and doctoral students]. 2010. No. 9(51). Pp. 99–101. (In Russian)
10. Andrianov V.I., Andronov A.V. Intellektual'nye sredstva obespecheniya informatsionnoy bezopasnosti avtomatizirovannykh sistem v usloviyakh neopredelennosti [Intelligent means of ensuring information security of automated systems in conditions of uncertainty]. *Zhurnal nauchnykh publikatsiy aspirantov i doktorantov* [Journal of scientific publications of postgraduates and doctoral students]. 2010. No. 8(50). Pp. 120–121. (In Russian)

INFORMATION ABOUT AUTHORS:
Sakharov D.V., PhD, Associate Professor of the Bonch-Bruevich Saint-Petersburg State University of Telecommunications;
Kovtsur M.M., PhD, Associate Professor of the Bonch-Bruevich Saint-Petersburg State University of Telecommunications;
Bakhtin D.V., Student of the Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

For citation: Sakharov D.V., Kovtsur M.M., Bakhtin D.V. Model of protection against exploits and rootkits with the following analysis and assessment of incidents. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 22–31. doi: 10.24411/2409-5419-2018-10284 (In Russian)

doi: 10.24411/2409-5419-2018-10285

БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ТИПА «УМНАЯ ЛОГИСТИКА» ДЛЯ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ СНАБЖЕНИЕМ

МИХАЙЛИЧЕНКО
Николай Валерьевич[1]

ПАРАЩУК
Игорь Борисович[2]

АННОТАЦИЯ

Обоснованы актуальность и объективная необходимость построения киберфизических систем типа «умная логистика» для автоматизированного управления снабжением. Сформулированы ключевые виды угроз безопасности, влияющей на функционирование систем такого класса. Для предотвращения этих угроз предложена гипотеза о целесообразности создания инфраструктуры «умной безопасности», которая будет опираться на традиционные системы логистической (включая транспортную) безопасности – системы физической безопасности для логистической инфраструктуры и системы кибербезопасности информационных, вычислительных и финансовых инфраструктур логистики. Предметом исследования является функциональное ядро обеспечения безопасности киберфизических систем типа «умная логистика» для автоматизированного управления снабжением – «умная» подсистема мониторинга и управления инцидентами безопасности. Целью работы является анализ и выработка новых направлений теоретических исследований и практических разработок в интересах обеспечения комплексной безопасности киберфизических систем «умная логистика». Рассмотрены сущность концепции и архитектуры подсистемы мониторинга и управления инцидентами комплексной безопасности, как взаимосвязанного комплекса взглядов, идей и принципов сбора, нормализации, хранения, обработки и визуализации больших массивов разнородных данных о событиях безопасности для противодействия различным угрозам «умной логистике». Предложены формулировки частных задач и возможные пути их решения, направленные на создание современных средств и методов мониторинга и управления инцидентами комплексной безопасности систем такого класса. Практическая значимость: представленный подход позволяет строить подсистемы мониторинга и управления инцидентами комплексной безопасности киберфизических систем типа «умная логистика» для автоматизированного управления снабжением на основе рационального сочетания особенностей и перечней решаемых интеллектуальных задач элементов сети встроенных устройств, способных к адаптации и использованию когнитивных технологий и технологий искусственного интеллекта.

КЛЮЧЕВЫЕ СЛОВА: киберфизическая система; комплексная безопасность; управление инцидентами; умная логистика; мониторинг; угроза.

Сведения об авторах:

[1]преподаватель Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, 23esn2008@rambler.ru

[2]д.т.н., профессор, Заслуженный изобретатель Российской Федерации, профессор Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, shchuk@rambler.ru

Для цитирования: *Михайличенко Н.В., Паращук И.Б.* Безопасность киберфизических систем типа «умная логистика» для автоматизированного управления снабжением // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 32–38. doi: 10.24411/2409-5419-2018-10285

Введение

Основой эффективного применения и ритмичного функционирования различных сложных организационно-технических и производственных структур — департаментов, конгломератов, промышленных и сырьевых групп (группировок), организаций и подразделений любых министерств и ведомств, включая силовые министерства, является их бесперебойное и регулярное снабжение. Снабжение осуществляется в рамках подсистем обеспечения и бывает техническим, материальным (сырье), финансовым, информационным, вещевым, артиллерийским (например, боеприпасы), медицинским, продовольственным и др.

Иными словами, осуществляется снабжение сырьем, товарами, полуфабрикатами и другими предметами материально-технического оснащения. Иногда говорят о двух ключевых видах снабжения — продовольственном и материально-техническом. Традиционно эти задачи решаются с помощью логистических систем. Тенденцией последних лет является построение и развитие подсистем «умной логистики». Системы такого класса относят к группе киберфизических систем (КФС) и предрекают им большое будущее.

В сущности, любая киберфизическая система (Cyber Physical Systems, CPS) — единая информационно-технологическая среда (пространство), обеспечивающая интеграцию вычислительных ресурсов в физические процессы [1–2], в нашем случае — в физические логистические процессы. Это техническая система, в которой взаимосвязаны вычислительные элементы и элементы физической природы, служащие источниками и потребителями информации [1]. Это система, обладающая непрерывной связью между своими вычислительными и физическими элементами, ее иногда сравнивают с робототехникой или сенсорными сетями.

Уже сегодня КФС активно функционируют, обеспечивая взаимодействие сенсоров, датчиков, оборудования и информационных подсистем в самых разнообразных областях — в космосе, автомобильной, химической промышленности, энергетике, здравоохранении и на транспорте. С учетом этого, одним из перспективных подходов к организации и автоматизированному управлению снабжением современные исследователи называют создание сложных компьютеризированных интеллектуальных систем типа «умная логистика». Примерами практического применения киберфизических систем с точки зрения «умной логистики», могут служить КФС, способные улучшить логистические процессы, обеспечивая обмен информацией реального времени между промышленным, складским и транспортным оборудованием для снабжения, цепочкой поставок, поставщиками (снабженцами), системами управления логистикой и клиентами. Кроме того, КФС типа «умная логистика» могут повышать эффективность этих процессов благодаря автоматическому мониторингу и контролю всего логистического процесса и адаптации логистики для удовлетворения предпочтений клиентов. Эти системы повышают прозрачность и управляемость цепочек поставок, улучшая отслеживаемость и безопасность снабжения.

Более того, в КФС типа «умная логистика», транспортные средства и инфраструктура снабжения могут взаимодействовать между собой, обмениваясь в реальном времени информацией о дорожном движении, загрузке складов и хранилищ, наличии запасов, местоположении средств снабжения и проблемах, предотвращая транспортные инциденты и дорожные пробки, повышая безопасность логистики и, в конечном итоге, экономя время и деньги.

Киберфизические системы типа «умная логистика»

Киберфизические системы типа «умная логистика» объединяют в себе кибернетическое начало, компьютерные (аппаратные) и программные технологии логистики, современные и взаимосвязанные логистические исполнительные механизмы, встроенные в среду снабжения и способные воспринимать изменения этой среды, обмениваться информацией, реагировать на них, самообучаться и адаптироваться.

Именно поэтому, КФС типа «умная логистика» занимают важное место в современном мире, наряду с «умным производством», «умным здравоохранением», «умной энергетикой» и другими Smart-технологиями, опирающимися на инновационные системы управления производством (АСУ ТП, SCADA-системы), «Интернет вещей» (Internet of Things), робото-технические системы, беспилотные летательные аппараты, беспилотные автомобили и др., включая системы военного назначения.

Иными словами, идею «умной логистики» («smart logistics», «логистика будущего»), рассматривают как одно из перспективных направлений развития современных КФС. Принято считать, что использование КФС типа «умная логистика» позволит существенно увеличить эффективность снабжения, автономность, адаптивность, надежность, эргономичность поставок СМТО, и, что самое главное — их безопасность [1–4]. С точки зрения «умной логистики», как инструмента «умной» и рациональной организации потоковых процессов с минимальными затратами трудовых и материальных ресурсов, ожидается, что данные усовершенствования расширят потенциал КФС в ряде направлений: беспилотный транспорт; внешнее вмешательство (предотвращение столкновений); точность (автоматизированная логистика); работа транспорта в опасных и недоступных средах; энергоэффективность (электромобили и гибридные транспортные средства); расширение способностей человека по управлению логистикой в целом, ее транспортными средствами и др.

Киберфизические системы типа «умная логистика» — это и «умные дороги» для снабжения (контроль покрытия), и единый диспетчерский центр системы «Платон» и табло с информацией о пробках на путях снабжения (дорогах) и уровне загруженности складов и терминалов и «умные» светофоры (включая светофоры на солнечных батареях) и система анализа транспортного потока (центр управления дорожным движением, включающий дорожные датчики и системы фото- и видеофиксации) и использование информационной логистической транспортной системы и управление парковочным, складским и погрузочным пространством и мониторинг параметров логистических (транспортных) потоков и внедрение динамических дорожных табло, систем видеоконтроля [5, 6]. Кроме того, это размещение электронных табло на складах, транзитных пунктах, внедрение и контроль единых электронных документов по логистике, систем мобильной оплаты за поставляемые средства материально-технического оснащения (СМТО), использование беспилотного грузового транспорта в «умной логистике», а также контроль нарушений правил логистики и дорожного движения, внедрение дистанционного весового контроля грузового транспорта, используемого для снабжения [7–9].

Таким образом, КФС типа «умная логистика» представляют собой конгломерат сетевых распределенных физических и кибернетических, логистических и транспортных инфраструктур. Они нацелены на обеспечение высокого качества снабжения и перевозок за счет применения инновационных технологий [10]. Очень важным является необходимость предусмотреть экологичное, экономичное и безопасное функционирование объектов «умной логистики» и использование систем жизнеобеспечения отраслевого транспорта и транспортной системы страны в целях эффективной логистики.

Киберфизические системы типа «умная логистика» должны включать в себя ряд ключевых подсистем: «умное планирование, распределение и перераспределение грузов», «умное дорожное движение», «умные грузоперевозки», «умное транспортное хозяйство», «умный топливозаправочный комплекс», «умное управление в сложных логистических и транспортных ситуациях» и «умная безопасность» [11].

При этом базовыми требованиями к организации «умной логистики» являются:

– поставка необходимого ассортимента средств материально-технического оснащения в достаточном количестве и высокого качества;

– ритмичность и своевременность завоза СМТО при соблюдении графика доставки;

– снижение количества посредников в каналах снабжения (доставки) с учетом эффективного использования транспортных средств и наличия фондов СМТО;

– минимизация затрат (трудовых и материальных) при организации и управлении логистикой;

– безусловная комплексная и «умная» безопасность организации и управления логистикой.

Требования, предъявляемые к комплексной и «умной» безопасности КФС типа «умная логистика» для автоматизированного управления снабжением, охватывают, помимо традиционной транспортной безопасности, все «умные» компоненты этой сложной КФС («умная» транспортная логистика, «умная» таможенная логистика, «умная» производственная логистика, «умная» логистика запасов, «умная» закупочная логистика (иногда именно ее называют логистикой снабжения), «умная» информационная логистика и «умная» складская логистика) и проникающим во все эти отрасли логистики и сферы интересов жизнедеятельности логистических систем [12].

Процесс автоматизированного логистического управления включает в себя различные составные части, обеспечивающие оптимальные результаты работы данной системы, но все большее значение приобретают вопросы защиты кибернетических и информационных ресурсов систем такого класса.

Сущность и направления обеспечения комплексной безопасности современных киберфизических систем типа «умная логистика» в интересах автоматизированного управления всеми видами снабжения

Эксперименты показывают, что по мере расширения связей, путей обмена информацией в рамках КФС подобного типа, причем связей, использующих открытые стандарты и протоколы робототехнических систем, технологии «Интернет вещей» (Internet of Things, IoT) или сенсорных сетей, рост рисков кибербезопасности, рисков информационной безопасности неизбежен, для защиты киберфизических систем типа «умная логистика» потребуется не только качественная и безопасная связь, но и системы управления учетными записями и системы контроля доступа.

«Умная безопасность» для «умной логистики» опирается на традиционные системы логистической (включая транспортную) безопасности — системы физической безопасности для логистической инфраструктуры и системы кибербезопасности информационных и вычислительных инфраструктур логистики, способные быстро реагировать на тревожные события, тем самым снижая уровень угроз.

Безопасность киберфизических систем типа «умная логистика» для автоматизированного управления снабжением основана на возможности подключения датчиков к единой «умной» системе безопасности и проведения мониторинга комплексной безопасности «умной логистики» в реальном времени. Это позволяет предвидеть и предот-

вращать негативные явления, коллизии в кибернетической сфере логистики, аварийные ситуации, отслеживать состояние транспортных сетей, складов и хранилищ, решать большой спектр задач на объектах логистики, следить за обстановкой, эффективно контролировать все жизненно важные объекты логистической инфраструктуры.

Проблемы безопасности «умной логистики» для автоматизированного управления снабжением — совокупность задач обеспечения безопасности стратегического управления материальными потоками (потоками СМТО, информационными и финансовыми потоками), задач комплексного использования совокупности методов и средств безопасности логистических систем и сетей, систем управления транспортом (дорожным движением), транспортных услуг, автоматизированных транспортных и складских предприятий, компьютеризированных систем грузовых перевозок, вплоть до каждого беспилотного либо «умного» автомобиля, «умного транспортного предприятия», «умного транспортного офиса» и отдельного человека, работающего или пользующегося услугами «умной логистики». Важно, что современные методы и средства мониторинга и управления инцидентами (МУИ) безопасности являются, на наш взгляд, основой обеспечения «умной безопасности» киберфизических систем типа «умная логистика» [13–14].

Основные направления исследований и практических разработок в интересах обеспечения комплексной безопасности КФС типа «умная логистика» для автоматизированного управления снабжением включают целый ряд этапов. При этом предшествует исследованиям детальный аналитический обзор современного научно-технического, нормативного и методического материала, затрагивающего данную научно-техническую проблему. Особое внимание должно быть уделено анализу существующих подходов, методов и алгоритмов современной и перспективной логистической (включая транспортную) безопасности, безопасности информационных и финансовых потоков, анализу самой концепции «умной логистики», анализу ее «умных» элементов, а также объединяющей их подсистемы «умной безопасности». Ключевое место должны занимать анализ и систематизация перечня угроз безопасности «умной логистики», анализ возможных атак на КФС типа «умная логистика», существующих моделей и методов МУИ.

Важная теоретическая задача — разработка концепции и архитектуры системы МУИ комплексной безопасности КФС типа «умная логистика», как взаимосвязанного комплекса взглядов, идей и принципов сбора, нормализации, хранения, обработки и визуализации больших массивов разнородных данных о событиях безопасности для противодействия различным угрозам «умной логистике». Концепция и архитектура системы МУИ комплексной безопасности должны опираться на современные подходы в области проектирования, создания и применения в логистике методов и программно-аппаратных средств многоуровневого и оперативного сбора, нормализации, хранения, обработки и визуализации больших массивов разнородных данных о событиях комплексной безопасности и управления ими.

В интересах МУИ комплексной безопасности «умной логистики» необходима разработка моделей, методов, методик, алгоритмов и программных средств проектирования встроенных устройств на базе интеллектуальных многофункциональных микроконтроллеров. Более того, понадобятся модели, алгоритмы и программные средства проектирования адаптивных, модульных, самонастраивающихся и масштабируемых сетей встроенных устройств для МУИ комплексной безопасности «умной логистики». Необходимы модели, методы и программные средства сбора и предобработки больших массивов гетерогенных данных от разнородных источников, нужны средства хранения больших массивов гетерогенных данных для МУИ комплексной безопасности «умной логистики». При этом хранение больших массивов данных МУИ может быть реализовано на основе методов и алгоритмов, предложенных в концепции распределенной файловой системы Hadoop (Hadoop Distributed File System, HDFS).

Наиболее важными и трудоемкими, на наш взгляд, являются научные и практические задачи по разработке моделей, методов, методик, алгоритмов и программных средств анализа данных и принятия решений по управлению инцидентами отдельно физической и кибернетической безопасности «умной логистики» на основе анализа больших массивов гетерогенных данных, а также по управлению комплексными инцидентами безопасности «умной логистики». Предлагается совместное, интегрированное и синергетическое объединение отдельных аспектов проблемы — конкретное воплощение совокупности методов, обобщенный перечень этапов многоуровневого, оперативного сбора, нормализации, хранения, обработки и визуализации больших массивов разнородных данных, получаемых в виде гетерогенного трафика от различных источников, и этапов управления инцидентами [13].

Современный уровень науки требует использования как стандартных, так и специально разработанных для этой цели нестандартных моделей и методов визуализации больших массивов гетерогенных данных МУИ комплексной безопасности «умной логистики», в том числе, на основе виртуальной и дополненной реальности. Необходима разработка экспериментального образца программно-аппаратного обеспечения для МУИ комплексной безопасности «умной логистики», программно-аппаратных стендов, имитирующих работу отдельных элементов инфраструктуры «умной логистики» [14].

Заключение

Таким образом, методы и средства обеспечения комплексной безопасности КФС типа «умная логистика», в конечном итоге, представляют собой технологию МУИ комплексной безопасности «умной логистики», которая будет базироваться на методах и алгоритмах проектирования встроенных систем и построения сети интеллектуальных встроенных устройств. Основная идея технологии МУИ комплексной безопасности «умной логистики» заключается в объединении особенностей (модульность, масштабируемость) и функциональностей элементов сети встроенных устройств, в объединении их способности к адаптации и использованию когнитивных технологий и искусственного интеллекта. Применение технологии и совокупности программно-аппаратных средств как единой системы МУИ комплексной безопасности должно осуществляться комплексно, на разных уровнях структуры «умной логистики», в автоматизированном и (или) автоматическом режиме (на верхнем уровне иерархии — обязательно с участием человека). Функциональная взаимосвязь — комплексные «умный мониторинг» и «умное управление инцидентами» в интересах «умной безопасности» (комплексной) для «умной логистики» — должны быть практически реализованы в рамках единого ситуационного центра «умной логистики» для города, региона, отрасли или страны.

Создание современных методов и средств обеспечения комплексной безопасности киберфизических систем типа «умная логистика» является прекрасным «полигоном» для применения и «обкатки» передовых научных достижений: когнитивных технологий и искусственного интеллекта для обработки данных, распределенной параллельной обработки больших данных, формального и визуального представления знаний о сложных событиях, онтологического моделирования данных о безопасности элементов «умной логистики», логического вывода на знаниях о безопасности, поддержки принятия решений и анализа защищенности информации.

Литература

1. Strategic Opportunities for 21st Century Cyber-Physical Systems: Workshop Report «Foundations for Innovation in Cyber-Physical Systems» (Chicago, IL, March 13–14, 2012). URL: http://events.energetics.com/NIST-CPSWorkshop/downloads.html (дата обращения 5.10.2019).

2. *Lee E.* Cyber Physical Systems: Design Challenges. EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2008–8. January 23, 2008. 10 p.

3. *Colombo A., Karnouskos S., Mendes J.* Factory of the future: A service-oriented system of modular, dynamic reconfigurable and collaborative systems // Artificial Intelligence Techniques for Networked Manufacturing Enterprises Management. Springer Series in Advanced Manufacturing. London: Springer, 2010. Pp. 459–481.

4. *Черняк Л. В*. Киберфизические системы на старте // Открытые системы. СУБД. 2014. № 2. С. 10–11.

5. *Faulin J., Grasman S., Juan A., Hirsch P.* Sustainable Transportation and Smart Logistics. Decision-Making Models and Solutions. 1st ed. Amsterdam Netherlands: Elsevier, 2018. 534 p.

6. *Kawa A.* SMART Logistics Chain // Intelligent Information and Database Systems: Proceedings of the 4th Asian conference on Intelligent Information and Database (ACIIDS2012) (Kaohsiung, Taiwan, March 19–21, 2012). Springer-Verlag Berlin Heidelberg, 2012. LNAI 7196, Part I. 2012. Pp. 432–438.

7. *Николаев В. С*. Умные города — будущее сегодня // Jet Info. 2015. № 10. С. 35–38.

8. *Дмитриев И.И., Кириллов А.М*. Умные дороги и Интеллектуальная транспортная система // Строительство уникальных зданий и сооружений. 2017. № 2 (53). С. 7–28.

9. *Комаров В.В., Гараган С. А*. Интеллектуальные задачи телематических транспортных систем и интеллектуальная транспортная система // T-Comm: Телекоммуникации и транспорт. 2012. Т. 6. № 4. С. 34–38.

10. *Алтухова Ю.В., Тонеян З.Г*. Интеллектуальные информационные системы в транспорте // Материалы докладов III региональной заочной научно-практической конференции «Интеллектуальные информационные системы: тенденции, проблемы, перспективы (ИИС-2015)» (Курск, 23 октября 2015 г.). Курск: Унив. кн.: Юго-Западный гос. ун-т, 2015. С. 19–21.

11. *Paul A., Chilamkurti N., Daniel A., Rho S.* Introduction: intelligent vehicular communications // Intelligent Vehicular Networks and Communications. Elsevier, 2017. Chapter 1. Pp. 1–20.

12. *Ruiz J., Desnitsky V., Harjani R., Manna A., Kotenko I., Chechulin A.* Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012) (Munich, German, 15–17 February 2012). IEEE, 2012. Pp. 261–268.

13. *Levshun D., Chechulin A., Kotenko I.* Design Lifecycle for Secure Cyber-Physical Systems based on Embedded Devices // Proceedings of the 2017 IEEE9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (Bucharest, Romania, 21–23 September, 2017). IEEE, 2017. Pp. 277–282.

14. *Котенко И.В., Паращук И.Б.* Анализ задач и потенциальных направлений разработки современных методов и средств обеспечения комплексной безопасности киберфизических систем типа «умный транспорт» // Научное обозрение. 2017. № 25. С. 26–30.

SECURITY OF CYBER-PHYSICAL SYSTEMS «SMART LOGISTICS» FOR AUTOMATED SUPPLY MANAGEMENT

NIKOLAI V. MIKHAILICHENKO
St. Petersburg, Russia, 23esn2008@rambler.ru

IGOR B. PARASHCHUK
St. Petersburg, Russia, shchuk@rambler.ru

KEYWORDS: cyber-physical system; integrated security; incident management; smart logistics; monitoring; threat.

ABSTRACT

The urgency and objective necessity of building cyber-physical systems such as «smart logistics» for automated supply management are substantiated. The key types of security threats affecting the functioning of systems of this class are formulated. To prevent these threats, the hypothesis of the feasibility of creating an infrastructure of «smart security», which will be based on the traditional system of logistics (including transport) security – physical security systems for logistics infrastructure and cyber-security information, computing and financial logistics infrastructure. The subject of the study is the functional core of the security of cyber-physical systems such as «smart logistics» for automated supply management – «smart» subsystem for monitoring and management of security incidents. The aim of the work is to analyze and develop new areas of theoretical research and practical development in order to ensure the integrated security of cyber-physical systems «smart logistics». The essence of the concept and architecture of the subsystem of monitoring and management of complex security incidents as an interrelated set of views, ideas and principles of collection, normalization, storage, processing and visualization of large amounts of heterogeneous data on security events to counter various threats to «smart logistics». The formulations of particular tasks and possible solutions aimed at the creation of modern tools and methods of monitoring and incident management of complex security systems of this class are proposed. Practical significance: the presented approach allows to build subsystems for monitoring and incident management of complex security of cyber-physical systems such as «smart logistics» for automated supply management based on a rational combination of features and lists of intellectual tasks of elements of the network of embedded devices capable of adaptation and use of cognitive technologies and artificial intelligence technologies.

REFERENCES

1. Strategic Opportunities for 21st Century Cyber-Physical Systems: Workshop Report "Foundations for Innovation in Cyber-Physical Systems" (Chicago, IL, March 13–14, 2012). URL: http://events.energetics.com/NIST-CPSWorkshop/downloads.html (date of access 5.10.2019)

2. Lee E. *Cyber Physical Systems: Design Challenges.* EECS Department, University of California, Berkeley, Technical Report No. UCB/EECS-2008–8. January 23, 2008. 10 p.

3. Colombo A., Karnouskos S., Mendes J. Factory of the future: A service-oriented system of modular, dynamic reconfigurable and collaborative systems. *Artificial Intelligence Techniques for Networked Manufacturing Enterprises Management. Springer Series in Advanced Manufacturing.* London: Springer, 2010. Pp. 459–481.

4. Chernyak L.V. Kiberfizicheskie sistemy na starte [Cyber-physical systems at the start]. *Open system. DBMS*. 2014. No. 2. Pp. 10–11. (In Russian)

5. Faulin J., Grasman S., Juan A., Hirsch P. *Sustainable Transportation and Smart Logistics. Decision-Making Models and Solutions.* 1st ed. Amsterdam: Netherlands: Elsevier, 2018. 534 p.

6. Kawa A. SMART Logistics Chain. *Intelligent Information and Database Systems: Proceedings of the 4th Asian conference on Intelligent Information and Database (ACIIDS2012)*, Kaohsiung, Taiwan, March 19–21, 2012. Springer-Verlag Berlin Heidelberg, 2012. LNAI 7196, Part I. 2012. Pp. 432–438.

7. Nikolayev V.S. Umnye goroda – budushhee segodnja [Smart city – future today]. *Jet Info*. 2015. No10. 2015. Pp. 35–38. (In Russian)

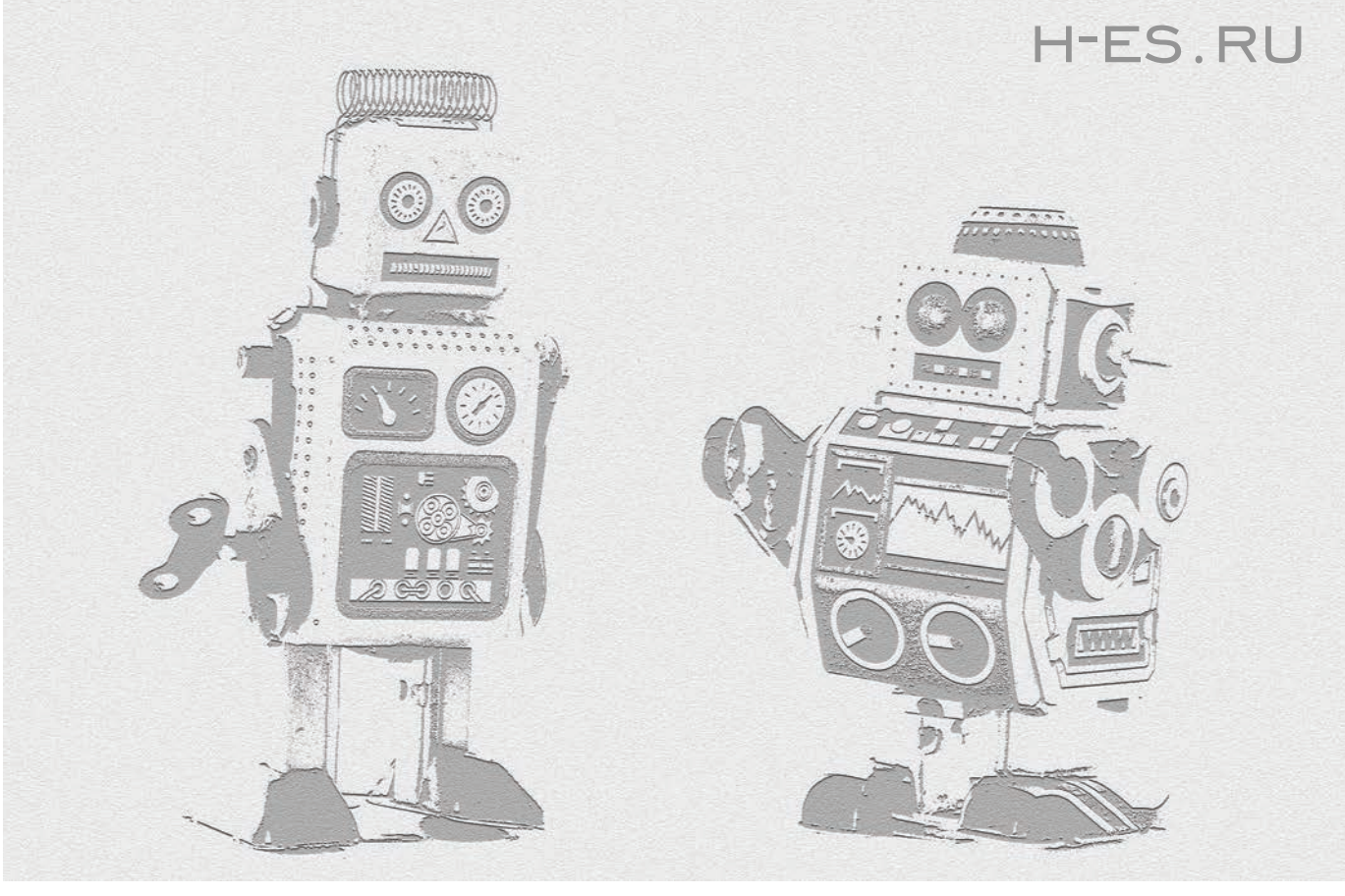
8. Dmitriev V.I., Kirillov A.M. Smart roads and Intellectual transport system. *Construction of Unique Buildings and Structures*. 2017. No. 2 (53). Pp. 7–28. (In Russian)

9. Komarov V.V., Garagan S.A. Intellectual tasks of telematic trans-

port systems and intellectual transport system. *T-Comm*. 2012. Vol. 6. No. 4. Pp. 34–38. (In Russian)
10. Altukhova Y.V., Toneyan Z.G. Intellektual'nye informacionnye sistemy v transporte [Intelligent information systems in transport]. [Intelligent information systems: trends, problems, prospects]. *Materialy dokladov III regional'noj zaochnoj nauchno-prakticheskoj konferencii "Intellektual'nye informacionnye sistemy: tendencii, problemy, perspektivy – IIS-2015"* [Proceedings of the III regional correspondence scientific-practical conference "Intelligent information systems: trends, problems, prospects – IIS-2015", Kursk, October 23, 2015]. Kursk: Univ. kn.: Southwest state University, 2015. Pp. 19–21. (In Russian)
11. Paul A., Chilamkurti N., Daniel A., Rho S. Introduction: intelligent vehicular communications. *In book: Intelligent Vehicular Networks and Communications*. Elsevier, 2017. Chapter 1. Pp. 1–20.
12. Ruiz J., Desnitsky V., Harjani R., Manna A., Kotenko I., Chechulin A. Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. *Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012)*, Munich, German, 15–17 February 2012. IEEE, 2012. Pp. 261–268.
13. Levshun D., Chechulin A., Kotenko I. Design Lifecycle for Secure Cyber-Physical Systems based on Embedded Devices. *Proceedings of the 2017 IEEE9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (Bucharest, Romania, 21–23 September, 2017). IEEE, 2017. Pp. 277–282.
14. Kotenko I.V., Parashchuk I.B. Analysis of tasks and potential directions of development of modern methods and means of complex security of cyber-physical systems of the "smart transport" type. *Science Review*. 2017. No. 25. Pp. 26–30. (In Russian)

INFORMATION ABOUT AUTHORS:
Mikhailichenko N.V., Lecturer of the Military Telecommunication Academy.
Parashchuk I.B., Ph.D., Full Professor, Professor of the Military Telecommunication Academy.

For citation: Mikhailichenko N.V., Parashchuk I.B. Security of cyber-physical systems «smart logistics» for automated supply management. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 32–38. doi: 10.24411/2409-5419-2018-10285 (In Russian)



doi: 10.24411/2409-5419-2018-10286

РАЗРАБОТКА МНОГОПАРАМЕТРИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНО-ПАРАЛЛЕЛЬНОЙ МАТРИЧНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СЕТИ

ПАВЛИКОВ
Сергей Николаевич[1]

УБАНКИН
Евгений Иванович[2]

КОЛОМЕЕЦ
Валерия Юрьевна[3]

ПЛЕННИК
Милена Денисовна[4]

АННОТАЦИЯ

В работе приведен анализ систем защиты сети от вредоносных программ. Предметом исследования является разработка метода комплексного анализа и оптимизации управления обработкой входной информации вычислительной сети в условиях взаимодействия с открытой не безопасной сетью при высокой неопределенности и рисках. Анализ состояния защиты вычислительной сети от входных вредоносных программных продуктов позволил определить проблему - высокая интенсивность и большая разнородность входной информации вычислительной системы в условиях взаимодействия с открытой сетью при неопределенностях и рисках снижает степень надежности защиты и функционирования вычислительной сети. Цель исследования – повышение эффективности метода комплексного анализа и оптимизации управления обработкой входной информации вычислительной системы в условиях высокой неопределенности и риска. Проблема - высокая интенсивность вирусных атак. Основным направлением исследований является создание новых и модификация существующих методов интеллектуального анализа входных данных с целью эффективного обнаружения аномалий, угрожающих функционированию объекта исследования. В работе показаны варианты построения, приведены критерии оптимизации. В работе рассматривается задача управления функционированием комплексной системы антивирусной защиты, состоящей из согласованных по уровням принятия решений нескольких антивирусных программ. Приведены результаты математического моделирования работы системы, приведен перечень взаимосвязанных необходимых для решения оптимизационных задач с выборам разновидностей антивирусных сканеров, настройки их пороговых значений, методики принятия частных решений по совокупности методов одинаковых уровней вероятностей первого и второго рода, методов с разными уровнями пороговых значений, а также методики принятия общего коллективного решения по назначенному критерию. Разработаны рекомендации оптимальных архитектуры и параметров антивирусного сканирования входного трафика. Анализ результатов экспериментальной проверки метода позволили определить условия и ограничения работы алгоритма. Разработаны рекомендации по настройке системы по количеству каналов, количеству уровней правил принятия коллективного решения в режиме обучения при размытых требованиях к входной модели вредоносного продукта и степени риска при использовании метода в реальных условиях. Таким образом, предложена структура многопараметрической последовательно-параллельной матричной системы защиты информационной сети, методы настройки и алгоритмы принятия решений с повышенным уровнем обнаружения вредоносных программ.

КЛЮЧЕВЫЕ СЛОВА: вирус; защита; сканер; сигнатура; динамические, статистические, методы защиты сети.

Сведения об авторах:

[1]к.т.н., профессор, профессор Владивостокского государственного университета экономики и сервиса, г. Владивосток, Россия, psn1953@mail.ru,

[2]к.т.н., доцент, доцент Морского государственного университета имени адмирала Г.И. Невельского, г. Владивосток, Россия, uei@inbox.ru,

[3]аспирант кафедры информационных технологий и систем Владивостокского государственного университета экономики и сервиса, г. Владивосток, Россия, lerospongebob@mail.ru,

[4]аспирант кафедры радиоэлектроники и радиосвязи Морского государственного университета имени адмирала Г.И. Невельского, г. Владивосток, Россия, milkatim@yandex.ru.

Для цитирования: *Павликов С.Н., Убанкин Е.И., Коломеец В.Ю., Пленник М.Д.* Разработка многопараметрической последовательно-параллельной матричной системы защиты информационной сети // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 39–47. doi: 10.24411/2409-5419-2018-10286

Объектом исследования является система защиты информационной сети от входных вредоносных программных продуктов (ВПП).

Предмет — разработка метода комплексного анализа и оптимизации управления обработкой входной информации вычислительной сети в условиях взаимодействия с открытой не безопасной сетью при высокой неопределенности и рисках.

Актуальность. Анализ состояния защиты вычислительной сети от входных вредоносных программных продуктов позволил определить проблему — высокая интенсивность и большая разнородность входной информации вычислительной системы в условиях взаимодействия с открытой сетью при неопределенностях и рисках снижает степень надежности защиты и функционирования вычислительной сети.

Цель исследования — повышение эффективности метода комплексного анализа и оптимизации управления обработкой входной информации вычислительной системы в условиях высокой неопределенности и риска.

Проблема — высокая интенсивность вирусных атак. Ни один известный антивирус не может гарантировать 100% защиту от вредоносных воздействий.

Основным направлением исследований является создание новых и модификация существующих методов интеллектуального анализа входных данных с целью эффективного обнаружения аномалий, угрожающих функционированию объекта исследования.

Компоненты усиливающие актуальность и обостряющие проблему:

– появление вирусов опережает создание антивирусных программ (АВП);

– ни одна АВП не гарантирует 100% обнаружения на этапе сигнатурного анализа;

– требуется согласование этапов и методов АВП в составе программного продукта одной лаборатории;

– требуется совместное решение антивирусной (АВ) защиты различных лабораторий и создание условий их совместного использования;

– сигнатуры скрыты, что приводит к избыточности затрат ресурсов, поэтому требуется стандартизация процедур АВП;

– метрологические требования разрабатываются и утверждаются локальными актами производителей, что приводит к несоответствию частных решений для различных АВП;

– количество АВП возрастает и базы данных (БД) требуют значительного увеличение памяти и времени поиска сигнатур;

– необходима стандартизация терминов в предметной области;

– полученные сигнатуры должны быть подтверждены другими независимыми лабораториями с указанием истории, условий их исследования и др.;

– вредоносные программные продукты создаются с возможностью маскировки и преобразования кодов, что снижает эффективность сигнатурного анализа.

– требуется принятие международных стандартов АВП, АВ защиты и к системам защиты.

Проблем много, но когда уровень угроз достигнет глобального масштаба потребуется консолидация и совместные скоординированные действия профильных центров информационной защиты вычислительных сетей.

Задачи:

1. Анализ входных угроз вычислительной системы;

2. Разработка метода комплексного анализа входной информации вычислительной системы в условиях высокой неопределенности и риска взаимодействия с открытой сетью;

3. Разработка устройства и алгоритмов управления обработкой входной информации;

4. Оценка эффективности разработанных алгоритмов и метода;

5. Разработка рекомендаций по применению новых и стандартизации известных АВП.

Задача исследования — совершенствования управления и принятия решений, с целью повышения эффективности АВ сканеров. Наиболее известными АВП являются:

1. Антивирус Dr. Web — надежная отечественная АВП, позволяющая с большой долей вероятности обнаруживать различные вредоносные программы https://www.sald.ru/.

2. Антивирус Касперского использует проактивные и облачные АВП для защиты от новых и неизвестных вредоносных программ. Обеспечивает базовую защиту в режиме реального времени https://www.kaspersky.ru/enterprise-security.

3. Антивирус NOD32 — эвристический анализ АВП, автоматическое сканирование персонального компьютера во время его простоя, проверка файлов непосредственно во время загрузки и возможность отменять установленные обновления. https://www.esetnod32.ru

4. Avast Pro Antivirus –эффективная защита при минимальной нагрузкой на системные ресурсы. Обеспечивает настройку параметров для качественной защиты ПК https://www.avast.ru.

5. Norton Security Standard, https://buy-static.norton.com.

Сравнительный анализ АВП показывает их достаточную эффективность для известных вредоносных программ. Все без исключения ведут интенсивный поиск новых направлений обнаружения, классификации и лечения внешних и внутренних угрожаемых программных продуктов.

Методами защиты от вредоносных программ являются предотвращения: поступления, атаки, деструктивных действий, таких как изменение файловой системы, ключей системного реестра, размножение и маскировки путем сокрытия и встраивания в другие процессы.

Все АВП реализуют методы сигнатурного, статистического, поведенческого и комплексного анализов.

Основными направлениями решения являются:

– применение комплексного метода анализа входного трафика;

– управлением распределением выполнения задач анализа входного трафика в условиях неоднородных вычислительных систем;

– управление принятием частных и комплексного решений по повышению эффективности функционирования информационной вычислительной системы в условиях высокой неопределенности входного трафика;

– моделирование, оптимизация и совершенствование управлением функционированием объекта и принятия решений корректирующих действий;

– формирование баз знаний по описанию угрожаемых и безопасных программных продуктов;

– определение перспективных технологий антивирусной защиты (АВЗ);

– разработка системы методов антивирусной защиты;

– разработка методик оценки эффективности разработанных алгоритмов, входящих в метод;

– разработка рекомендаций по построению системы и применению технического решения;

– разработка метрологического и др. обеспечения систем АВЗ.

Сложность направления заключается в расплывчатой классификации продуктов и технологий АВЗ.

Тема исследования достаточно широко представлена в информационных источниках [1–5].

Анализ публикаций и патентной информации показал, что имеются направления исследований, еще не достаточно освещенных в литературе [6–8].

Среди рассматриваемых технологий:

– комплексное применение в АВЗ от вирусных атак с использованием коллективного принятия решения на основе частных выводов экспертных подсистем;

– применение многоканальной обработки;

– использовании широкого диапазона глубин антивирусного сканирования;

– адаптивных алгоритмов принятия частных и общих решений;

Применение позволит повысить эффективность, надёжность работы в меняющихся условиях и ресурсных ограничениях. Совместное использование различных, зарекомендовавших себя АВП в системе для достижения единой цели позволяет получать синергетический эффект.

Предложено новое техническое решение, описанное в [9–10], при этом характеризуется рядом недостатков: увеличение ёмкости требуемых ресурсов, возникновения несогласованности уровней принятия решений для различных каналов.

Модель построения антивирусной сети приведена на рис. 1. Матрица размещения различных АВП представлен на рис. 2, где в столбце размещены АВП одного типа, например лаборатории Касперского, Данилова и др. По строкам размещены АВП с различными, возрастающими порогами

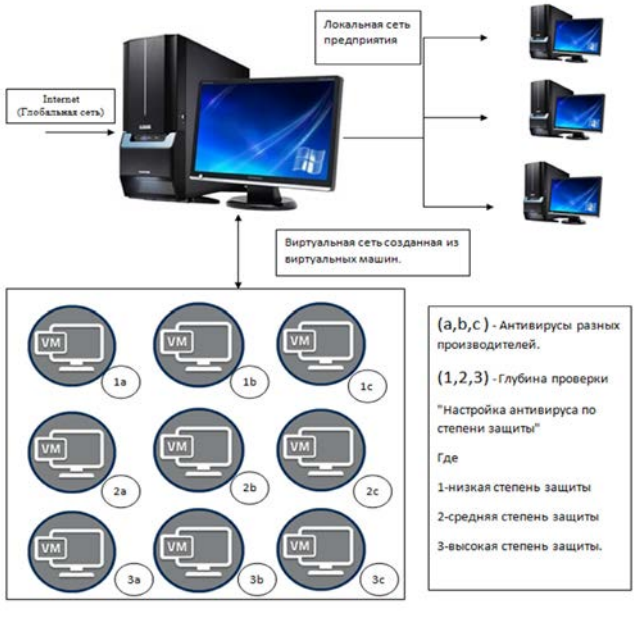


Рис. 1. Модель построения антивирусной сети приведена

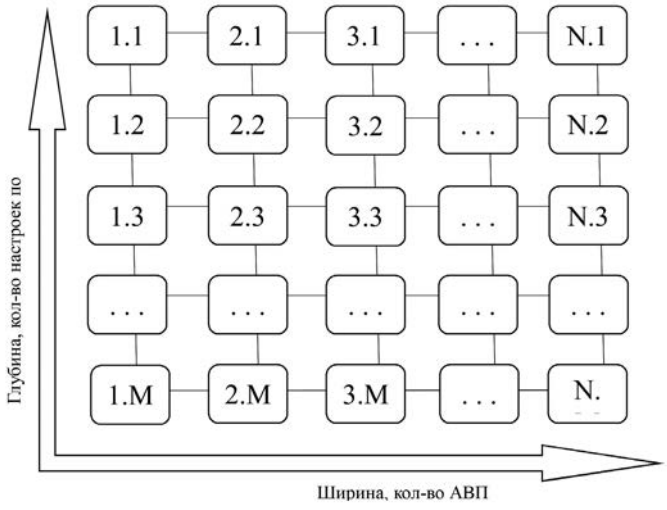


Рис. 2. Матрица антивирусной сети

принятия решения по обнаружению, при этом частные решения АВП первой строки будут характеризоваться низким порогом, высокой вероятностью ложной тревоги и высокой вероятностью правильного обнаружения. Вторая и последующие строки характеризуются снижением вероятности ложной тревоги и увеличением вероятности пропуска вредоносной программы.

Промежуточные решения коллективом АВП по строкам и по столбцам позволяют учесть особенности сигнатур АВ сканеров при стабилизации вероятности порогов для выбранной строки.

Особенности частных решений при изменении порога принятия решения учтены в работе алгоритма с группой АВП одного производителя, но при различных настройках порога принятия решений.

Алгоритм принятия промежуточного решения по результатам частных решений АВП только по строкам или только по столбцам матрицы приведен на рис. 3 и 4 соответственно.

Техническое решение приведено на рисунке 6 и относится к области защиты информации и оптимизации режимов функционирования программного обеспечения и может быть использована в домашних персональных компьютерах, серверах, а также в ЭВМ, применяемых на производстве. Работает устройство следующим образом. Входной программный продукт (ПП) поступает на первый вход коммутатора 3, который является входом предлагаемого устройства, после коммутации ПП со второго выхода коммутатора 3 передаётся параллельно на антивирусные блоки 1, выходы которых соединены с соответствующими входами многоканального разъема коммутатора 4. С выходов коммутатора 4 посредством блоков 5 и 6 информация

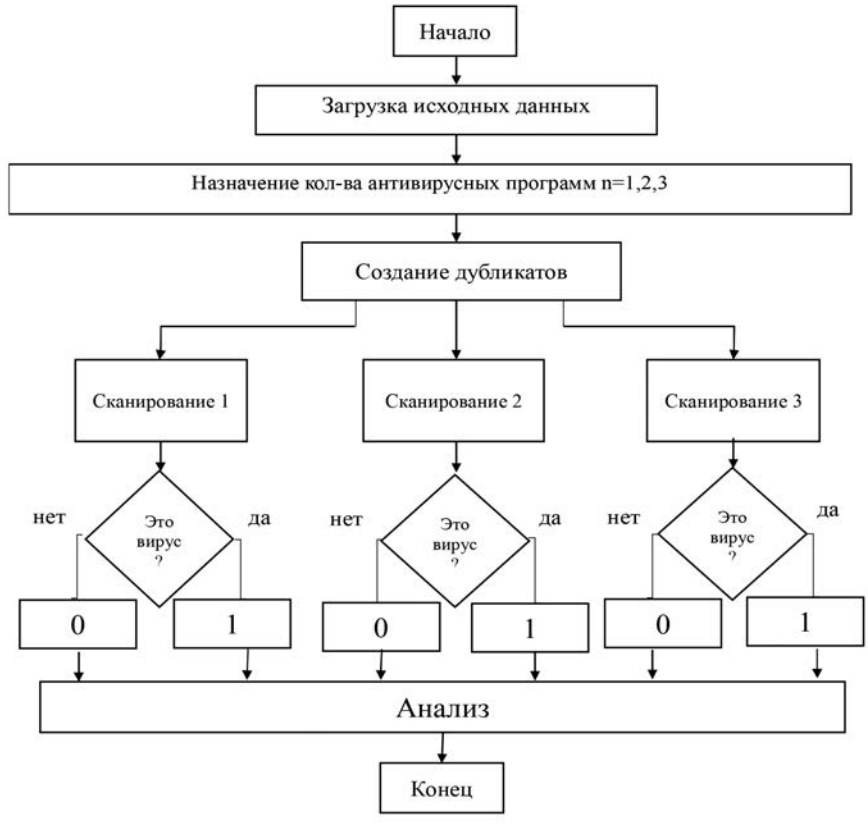


Рис. 3. Алгоритм принятия промежуточного решения по результатам частных решений АВП только по строкам

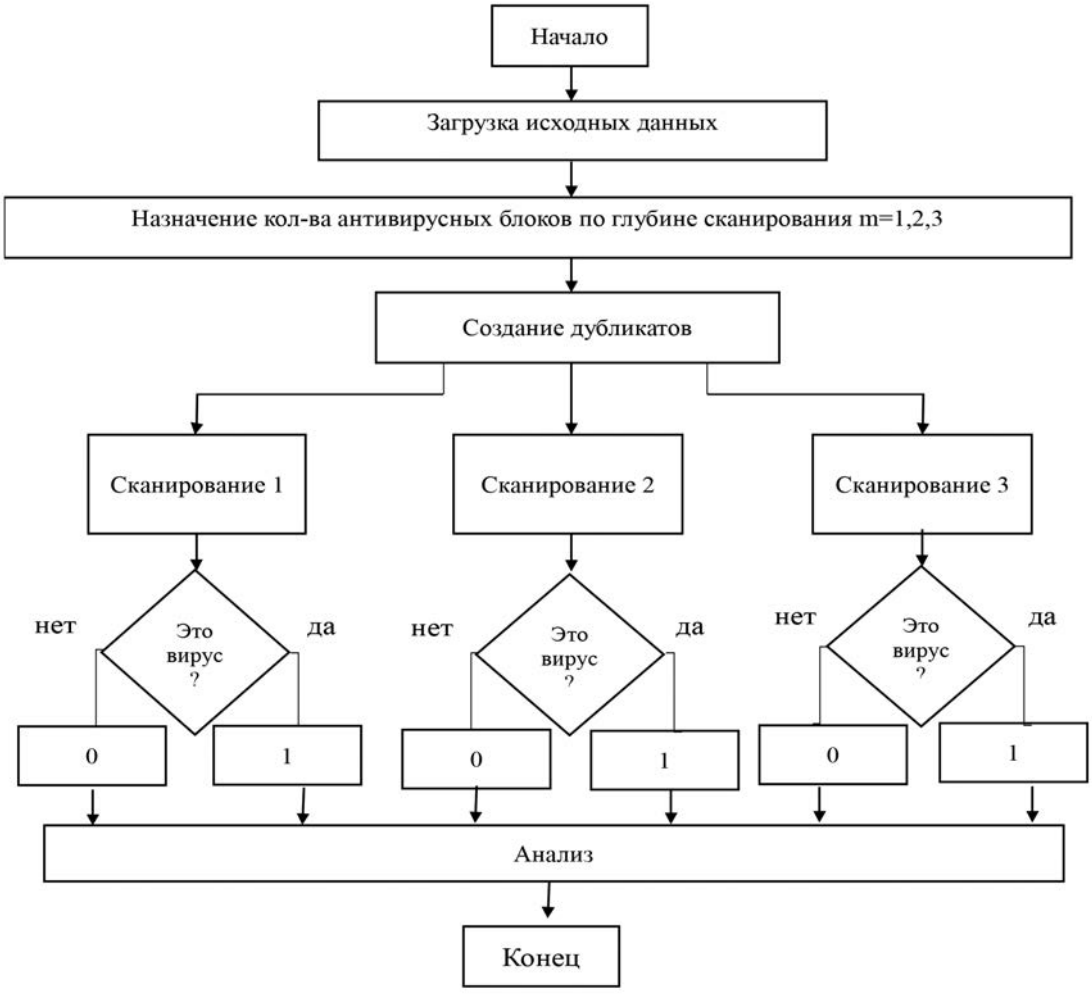


Рис. 4. Алгоритм принятия промежуточного решения по результатам частных решений АВП только по столбцам матрицы

передается в блок 7 принятия общего решения, который соединен с блоком управления 8. Первый выход управляющего блока 8 соединен со вторым входом коммутатора 4. С второго выхода блока 8 на второй вход блока 5 принятия коллективного решения поступают управляющие сигналы, сформированные с учетом частных решений антивирусных блоков 1, размещенных по строкам, в то же время третий выход блока управления 8 передает управляющие сигналы, сформированные с учетом частных решений антивирусных блоков 1, размещенных по столбцам, на второй вход блока 6 принятия коллективного решения, а четвертый выход блока управления 8 передает управляющие сигналы на второй вход коммутатора 3.

При этом первый разъём блока управления 8 через первый разъем модуля 2 обнаружения антивирусных систем направляет в антивирусные блоки 1 управляющие сигналы, задающие и контролирующие настройки и режимы их работы, и передает контрольную информацию в блок управления 8. В случае возникновения необходимости блок 8 через модуль 2 меняет антивирусные программы в антивирусных блоках и осуществляет подключение, отключение и настройку глубины сканирования с учетом результативности функционирования конкретных антивирусных блоков в сравнении с другими антивирусными блоками в предыдущий период работы. Результаты принятия частных решений антивирусных программ используются для выработки коллективных решений по строкам и столбцам матрицы, а затем коллективные решения участвуют в выработке общего решения. Блок управления 8 анализирует результативность обнаружения вредоносного программного продукта (вируса) антивирусными блоками путем сравнения частных решений с коллективными решениями по группам, по строкам и по столбцам, а также с общим решением и вырабатывает сигналы изменения и уточнения весовых коэффициентов учета частных решений в коллективных (например, с шагом 0,0001) решени-

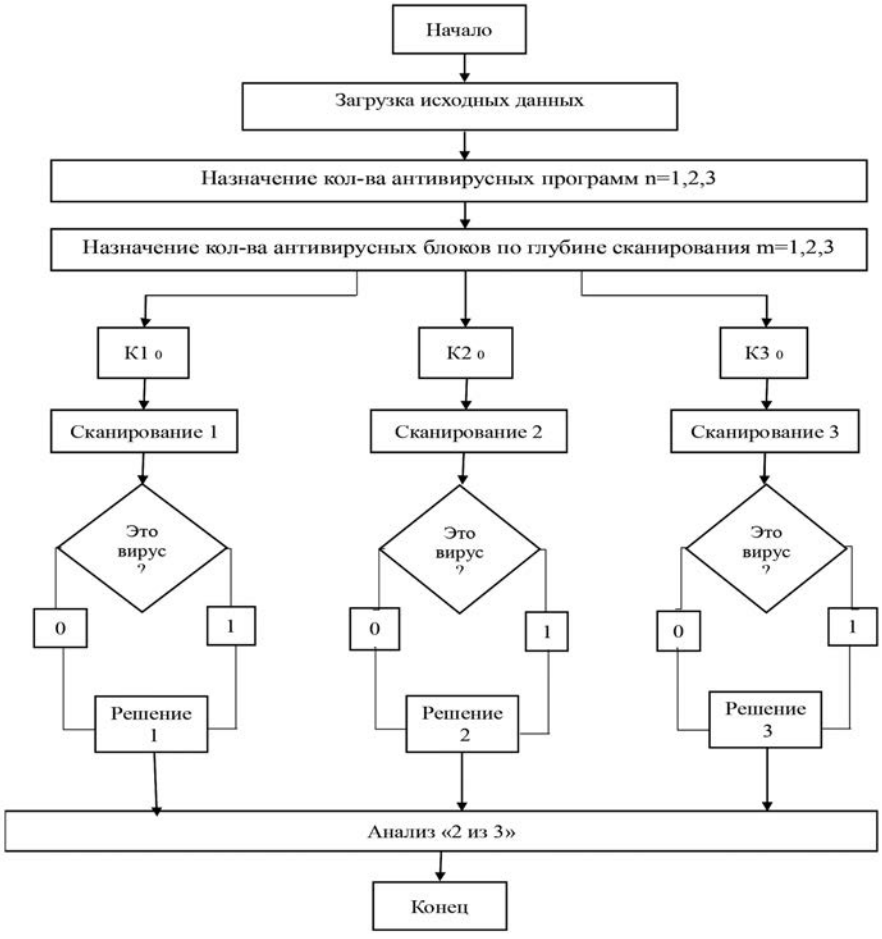


Рис. 5. Алгоритм принятия решения по результатам частных решений матрицы АВП

ях и коллективных решений в общем (например, с шагом 0,001); путем многократных сравнений адаптирует процесс принятия решения к особенностям вируса с учетом результативности антивирусных программ с различными порогами принятия решений.

В результате сравнения и анализа результативности система формирует уточненные весовые коэффициенты в блоках принятия коллективных решений по строкам и столбцам и общего решения.

С помощью обучающей выборки настраивают систему на определенный класс вирусов.

При поступлении на вход нового вируса система проводит многоуровневое сканирование разными АВП с разными совокупностями признаков, что позволяет повысить надежность обнаружения при заданных уровнях ошибочного решения. Антивирусные программы размещены в виртуальных, причем обособленных друг от друга, процессорных модулях и управляются блоком управления 8 через модуль 2. В случае, если установлено, что входной программный продукт не является вирусом, блок управления 8 подает разрешающий сигнал на его передачу на выход устройства, которым является первый выход коммутатора 3.

Для проверки работоспособности предложенного технического решения разработана комплексная программа обнаружения и оценки вирусного заражения компьютера []. Программа предназначена для антивирусной защиты персонального компьютера, компьютерной сети. При обнаружении вредоносной программы в результате использования нескольких антивирусных программ с различными возможностями обнаружения вирусов она имитирует формирование коллективного решения и обеспечивает оценку степени соответствия между частными решениями антивирусных программ и выработанным коллективным решением, а также может применяться для адаптации весовых коэффициентов при принятии коллективного решения в системе антивирусной защиты. В итоге программа обеспечивает выполнение следующих функций:

– имитацию частных решений антивирусных программ;

– принятие коллективного решения;

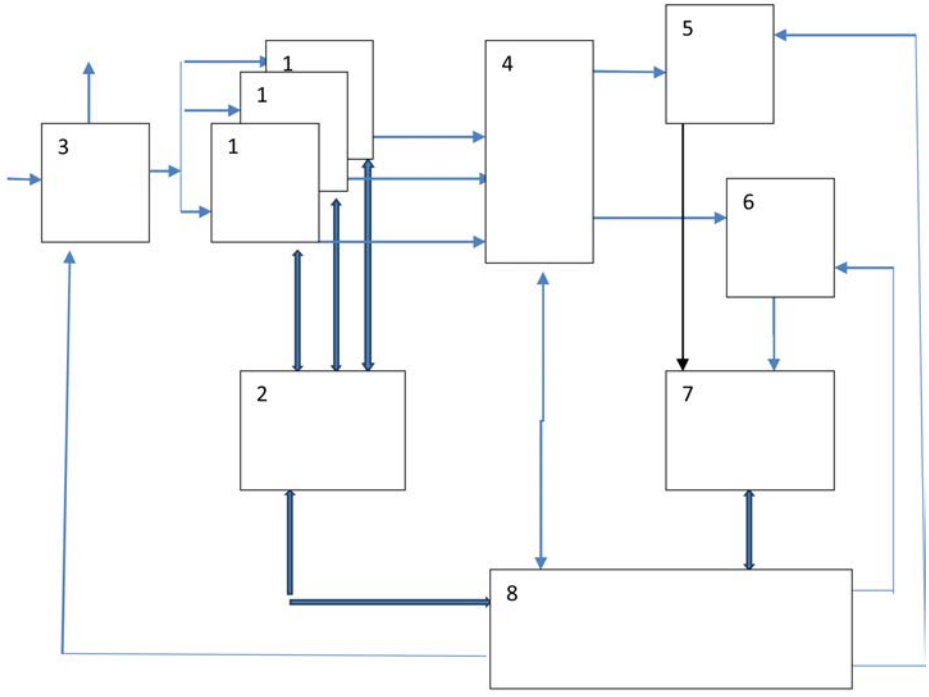


Рис. 6. Система адаптивного управления пакетом антивирусных программ, где обозначены:
1 – антивирусные блоки, 2 – модуль обнаружения анивирусных систем, 3, 4 – коммутаторы,
5 и 6 – блоки принятия чатных решений, 7 – блок принятьия общего решения, 8 – блок управления

– сравнение результатов частных решений с коллективным;

– адаптацию весовых коэффициентов алгоритма принятия коллективного решения;

– индикацию проученных результатов.

Предлагаемая система адаптивного управления пакетом антивирусных сканеров организована таким образом, чтобы достичь эффекта, превышающего суммарный эффект отдельных антивирусных программ. Совместное использование нескольких АВП с различными уровнями принятия решений относительно обнаружения вируса позволяет использовать набор признаков обнаружения (каждая АВП ранее обновлена и актуализирована) с различными уровнями сканирования, что обычному пользователю не представляется возможным выполнить. В такой ситуации разработчикам вирусов труднее создать программный продукт, противостоящий множеству АВП.

Литература

1. *Петров А. Ю.* Эффективные стратегии вирусной защиты // Информатизация образования и науки. 2010. № 4(8). С. 66–76.

2. *Назаров А. Н.* Синтез функций защиты от кибер-атак // T-comm: Телекоммуникации и транспорт. 2017. Т. 11. № 9. С. 80–85.

3. *Назаров А. Н.* Оценка защищенности от информационных атак // Телекоммуникации. 2016. № 5. С. 23–33.

4. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. 4-е изд. СПб.: Питер, 2010. С. 871–875.

5. *Язов Ю. К., Соловьев С. В.* Защита информации в информационных системах от несанкционированного доступа. Воронеж: Кварта, 2015. С. 357.

6. Патент РФ № 2453917. Система и способ для оптимизации выполнения антивирусных задач в локальной сети / Тихомиров А. В., Кульга А. А. Заявл. 30.12.2010. Опубл. 20.06.2012. Бюл. № 17. 30 р.

7. Патент РФ № 2012142156. Способ защиты компьютерной сети от вредоносного программного обеспечения / Ниемеля Я., Хюппёнен М., Кенгез С. Заявл.: 15.03.2011. Опубл.: 22.09.2011. Бюл. № 11. 4 с.

8. Патент РФ № 2527738. Способ обезвреживания вредоносных программ, блокирующих работу ПК / Богданов Д. Е. Заявл.: 24.04.2013. Опубл.: 10.09.2014. Бюл. № 25. 13 с.

9. Патент РФ № 179369. Система адаптивного управления пакетом антивирусных сканеров / Павликов С. Н., Коломеец В. Ю., Котович Е. Е., Стволовая А. К., Степанушкин Л. В.,Динкилакер В. В. Заявл. 21.08.2017. Опубл. 11.05.2018. Бюл. № 14. 9 с.

10. Свидетельство о государственной регистрации программы для ЭВМ № 2017619669. Комплексная антивирусная программа / Павликов С. Н., Коломеец В. Ю., Котович Е. Е. Заявл. 05.07 2017. Опубл. 01.09. 2017.

DEVELOPMENT MULTI-PARAMETERIC CONSENOY-SAPRICEMATIC MATRIX SYSTEM OF INFORMATION NETWORK

SERGEJ N. PAVLIKOV,
Vladivostok, Russia, psn1953@mail.ru

EVGENIY I. UBANKIN,
Vladivostok, Russia, uei@inbox.ru

VALERIA U. KOLOMEETS
Vladivostok, Russia, lerospongebob@mail.ru

MILENA D. PLENIK
Vladivostok, Russia, milkatim@yandex.ru

KEYWORDS: virus; protection the scanner signatures dynamic, statistical, network protection methods.

ABSTRACT

The work provides an analysis of the network's systems to protect against malware. The subject of the study is the development of a method of integrated analysis and optimization of the management of the processing of input information of the computer network in the context of interaction with an open and unsafe network with high uncertainty and risks. Analysis of the state of protection of the computer network from input malicious software products allowed to identify the problem - high intensity and high heterogeneity of the input information of the computer system in the context of interaction with the open network uncertainties and risks reduces the reliability of the protection and operation of the computing network. The aim of the study is to improve the effectiveness of the integrated analysis and optimization of the management of the processing of input information of the computer system in conditions of high uncertainty and risk. The problem is the high intensity of viral attacks. The main focus of research is the creation of new and modificational existing methods of intelligent analysis of input data in order to effectively detect anomalies that threaten the functioning of the research facility. The work shows the options for construction, the criteria for optimization. The work examines the task of managing the operation of a comprehensive antivirus protection system, consisting of agreed on the decision levels of several antivirus programs. The results of mathematical modeling of the system are given, a list of interconnected tasks necessary for solving optimization problems with the selection of varieties of antivirus scanners, setting their thresholds, methods of adoption private decisions on the combination of methods of the same levels of probability of the first and second kind, methods with different levels of thresholds, as well as methods of making a common collective decision on the assigned criterion. Recommendations for the optimal architecture and parameters of antivirus scanning of input traffic have been developed. Analysis of the results of the experimental test of the method allowed to determine the conditions and limitations of the algorithm. Recommendations have been developed on how many channels the system has been set up, the number of levels of collective decision-making rules in training mode, with blurred requirements for the input model of the malicious product, and the degree of risk when using the method in real-world conditions. Thus, the structure of the multi-parametric serial-parallel matrix system of information network protection, customization methods and decision-making algorithms with an increased level of detection of malware is proposed.

REFERENCES

1. Petrov A.Y. Effective strategies for antivirus. *Education and Science Information*. 2010. No. 4 (8). Pp. 66–76.
2. Nazarov A.N. Syntesz of security functions against cyber-attacks. T-comm. Vol. 11. No. 9. Pp. 80–85.
3. Nazarov A.N. Assessment of security from information attacks. *Telekommunikatsii* [Telecommunications]. 2016. No. 5. Pp. 23–33.
4. Olifer V.G., Olifer N.A. Computer Networks. Principles, technologies, protocols: Textbook for universities. 4th ed. St. Petersburg: Peter, 2010. Pp. 871–875.
5. Yazov Y.K., Solovyov S.V. *Protecting information in information systems from unauthorized access*. Voronezh: Quart, 2015. Pp. 357. 440 p.
6. Patent RF 2453917. System and method for optimising execution of antivirus tasks in local area network. Tikhomirov A.V., Kulaga A.A. Declar. 30.12.2010. Publ. 10.06.2008 20.06.2012. Bull. 17.
7. Patent 2012142156. A way to protect your computer network from malicious software. Niemel Ja., Huppyonen M., Kenges C. Declar. 15.03.2011. Publ. 22.09.2011. Bull. № 11. 4 p. (In Russian)
8. Patent RF 2527738. Method of neutralising malware blocking pc operation using separate device. Bogdanov D.E. Declar. 24.04.2013. Publ. 10.09.2014. Bull. 25. 13 p.

9. Patent RF 179369. Sistema adaptivnogo upravleniya paketom antivirusnyh skanerov [Adaptive control system package antivirus scanners]. Pavlikov S.N., Kolomeec V. Yu., Kotovich E.E., Stvolovaya A.K., Stepanushkin L.V., Dinkilaker V.V. Declar. 21.08.2017. Publ. 11.05.2018. Bull. 14. 9 p.
10. Certificate of state registration of the computer program No. 2017619669. Kompleksnaya antivirusnaya programma [Comprehensive antivirus software]. Pavlikov S.N., Kolomeec V. Yu., Kotovich E.E. Declar. 05.07.2017. Publ. 01.09. 2017.

INFORMATION ABOUT AUTHORS:
Pavlikov S.N., PhD, Full Professor, Professor of the Vladivostok state University of Economics and Service;
Ubankin E.I., PhD, Docent, Assistant Professor of the Vladivostok state University of Economics and Service;
Kolomeets V.U., Postgraduate student of the Vladivostok state University of Economics and Service;
Plenik M.D., Postgraduate student of the Vladivostok state University of Economics and Service.

For citation: Pavlikov S.N., Ubankin E.I., Kolomeets V.U., Plenik M.D. Development multi-parameteric consenoy-sapricematic matrix system of information network. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 39–47. doi: 10.24411/2409-5419-2018-10286 (In Russian)

doi: 10.24411/2409-5419-2018-10287

РАСЧЕТ МНОГОКАНАЛЬНОЙ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ С ПРЕРЫВАНИЯМИ И ГИПЕРЭКСПОНЕНЦИАЛЬНЫМИ РАСПРЕДЕЛЕНИЯМИ ВРЕМЕН ОБРАБОТКИ ЗАЯВОК И ПЕРИОДА НЕПРЕРЫВНОЙ ЗАНЯТОСТИ

ХАБАРОВ
Роман Сергеевич[1]

ХОМОНЕНКО
Анатолий Дмитриевич[2]

АННОТАЦИЯ

Предложен численный метод расчета стационарного распределения числа заявок для многоканальных систем массового обслуживания с абсолютным приоритетом, основанный на аппроксимации гиперэкспоненциальным распределением периода занятости объединенного потока классов с более высокими приоритетами. Из соображений обеспечения приемлемых характеристик точности и трудоемкости предполагается, что время обслуживания заявок каждого класса также представлено гиперэкспоненциальным распределением с заданными параметрами. При таком подходе расчет системы с множеством классов заявок производится последовательным расчетом систем с двумя классами – объединенным потоком заявок в качестве первого класса, и исследуемым, представляемым вторым. Количество заявок в очереди и на обслуживании фиксируется только для заявок второго класса. Предложен метод нахождения начальных моментов периода непрерывной занятости для заявок первого класса на основе длительности интервала с момента полного занятия каналов заявками первого класса до момента первого окончания обслуживания одной из заявок и численного интегрирования по полуоси с весом Чебышева-Лагерра. Представлен пример диаграмм условных интенсивностей переходов между состояниями системы по прибытии и обслуживанию для каждого из классов заявок для 2-х канальной системы массового обслуживания. Показан способ расчета системы на основе итерационного метода Такахаси-Таками. Поскольку оперативность прохождения заявок первого класса не зависит от прохождения заявок менее приоритетных классов, для расчета стационарного распределения числа заявок первого класса применяются известные численные методы итерационного типа для многоканальных систем с гиперэкспоненциальным распределением времени обслуживания без приоритетов. Метод реализован на языке программирования высокого уровня C#, представлен пример расчета стационарного распределения числа заявок для 2-х и 3-х канальной системы массового обслуживания, выполненный с помощью предложенного метода и имитационной модели. Получена достаточно высокая степень согласованности результатов.

КЛЮЧЕВЫЕ СЛОВА: вирус; теория очередей; многоканальные системы массового обслуживания; приоритетные дисциплины обслуживания; абсолютный приоритет; период непрерывной занятости.

Сведения об авторах:

[1]адъюнкт Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, xabarov1985@gmail.com

[2]д.т.н., профессор, заведующий кафедрой Петербургского государственного университета путей сообщения Императора Александра I, профессор Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, khomon@mail.ru

Для цитирования: *Хабаров Р.С., Хомоненко А.Д.* Расчет многоканальной системы массового обслуживания с прерываниями и гиперэкспоненциальными распределениями времен обработки заявок и периода непрерывной занятости // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 48–9. doi: 10.24411/2409-5419-2018-10287

Введение

Модели систем массового обслуживания (СМО) часто используются на этапе проектирования сложных систем для обоснования характеристик их производительности. Примерами таких систем являются центры обработки данных, морские и речные порты, лечебные учреждения, автоматические телефонные станции и др.

Особое значение модели СМО имеют при анализе функционирования вычислительных систем и сетей. С учетом требований производительности, надежности, а также организации технического обслуживания большинство узлов вычислительных систем и сетей является многоканальными. Поступающие в такие системы задачи, как правило, различаются по важности, трудоемкости, а также требованиям по оперативности обработки, что приводит к введению приоритетных дисциплин обслуживания в узлах. Считается, что предположение о экспоненциальном времени обслуживания для большинства реальных систем неверно. Таким образом, для анализа вычислительных систем следует использовать модели неэкспоненциальных СМО с многоканальными узлами и приоритетными дисциплинами обслуживания.

Расчет таких систем связан с определенными сложностями. Несмотря на то, что для одноканальных приоритетных систем массового обслуживания методы расчета представлены в многочисленных работах [1–4], нахождение точного решения для многоканального случая до сих пор не получено.

В большинстве работ, посвященным многоканальным СМО с приоритетами, исследуются модели с экспоненциальным обслуживанием M/M/n [5–8]. В [9] получены аппроксимации для средних времен ожидания СМО вида M/D/n с относительным приоритетом. Моделям с неэкспоненциальным распределением времени обслуживания, идентичным для каждого класса, посвящены работы [10–14]. Лишь единичные работы [13–14] рассматривают СМО с различными временами обслуживания. На основе инвариантов отношения в [15] предложено приближенное решение для средних времен ожидания. Идея заключается в применении символической пропорции между показателями систем массового обслуживаниям некоторых классов.

В [16–17] предложены методы численного расчета для многоканальных СМО с абсолютным и относительным приоритетом, основанный на аппроксимации периода полной непрерывной занятости. Получены решения для следующих случаев:

– время обслуживания заявок для всех классов распределено по экспоненциальному закону;

– время обслуживания одного из классов является произвольным и аппроксимируется гиперэкспоненциальным распределением второго порядка, а другого — по экспоненциальному закону.

В настоящей статье предлагается численный расчет стационарных вероятностей наличия в системе заявок для СМО с абсолютным приоритетом и произвольным распределением времени обслуживания для обоих классов заявок, аппроксимируемым с помощью гиперэкспоненциального распределения.

Общее описание метода

При введенных предположениях оперативность прохождения заявок r-го класса не зависит от прохождения заявок менее приоритетных классов $r+1,\ldots, k$. С точки зрения влияния на обслуживание r-заявок заявки классов $1,\ldots, r-1$ эквивалентны и могут быть объединены в один класс $\bar{r}$. Поток заявок класса $\bar{r}$ является пуассоновским с интенсивностью $\lambda_{\bar{r}} = \sum_{i=1}^{r-1}\lambda_i$. Для объединенного потока найдем усредненные моменты обслуживания согласно

$$b_j^{\bar{r}} = \frac{1}{\lambda_{\bar{r}}}\sum_{i=1}^{r-1}\lambda_i b_j^i.$$

Аппроксимируем времена обслуживания заявок объединенного потока и исследуемого одним из распределений фазового типа. Из соображений обеспечения приемлемых характеристик точности и трудоемкости воспользуемся для этого гиперэкспоненциальным распределением. Параметры гиперэкспоненциального распределения для объединённого потока $\{u_i, \chi_i\}, i=\overline{1,2}$, для исследуемого — $\{\nu_i, \gamma_i\}, i=\overline{1,2}$ Теперь будем анализировать СМО $M^{[2]}/H_2^{[2]}/n/\infty/f_a$ — с двумя приоритетными классами заявок. Здесь классу 2 соответствует исследуемый поток, а классу 1 — объединенный поток.

Для оценки характеристик прохождения заявок 1-го класса приоритетности нам достаточно рассмотреть СМО типа $M/G/n/\infty$ Решение для таких систем может быть получено известными методами [18–20]. Попытка непосредственно составить уравнения баланса с целью прохождения заявок 2-го класса упирается в проблему существенного роста размерности задачи.

Проблема размерности разрешима следующим образом. При определении состояния СМО типа $M^{[2]}/H_2^{[2]}/n/\infty/f_a$ количество заявок в очереди и на обслуживании будем фиксировать только для заявок 2-го класса. Для 1-го класса ограничимся указанием количества обслуживаемых заявок $l_i = \overline{0,n-1}$. При $l_i = n$ считаем, что система находится в состоянии полной занятости всех каналов обслуживания заявок 1-го класса приоритетности. Чтобы учесть влияние заявок 1-го класса на прохождение заявок 2-го класса, достаточно определить параметры распределения периода полной непрерывной занятости (ППЗК) заявками 1-го класса.

Пусть T_{1n} — длительность интервала с момента полного занятия каналов заявками 1-го класса до момента

первого окончания обслуживания одной из заявок, а $T_{ПЗ}$ — длительность ППЗК заявками 1-го класса. Обозначим $b_n(s)$ и $\pi_n(s)$ — ПЛС распределения длительностей интервалов T_{1n} и $T_{ПЗ}$ соответственно.

Интерпретируем s как параметр простейшего потока «катастроф». Тогда $b_n(s)$ и $\pi_n(s)$ можно истолковать как вероятности отсутствия катастроф за случайное время обслуживания и ПНЗ соответственно. Назовем заявку «плохой», если в течение открываемого ею ПНЗ происходит катастрофа. Простейший поток таких заявок будет иметь параметр $\lambda_1(1-\pi_n(s))$, а суммарный поток неблагоприятных событий — параметр $(s+\lambda_1(1-\pi_n(s)))$

Таким образом, для ПЛС искомого распределения справедливо следующее функциональное уравнение

$$\pi_П(s)= b_n\,(s+\lambda_1-\lambda_1\pi_П(s)).$$

Данное уравнение позволяет выразить начальные моменты $\{\pi_i\}$ требуемого нам распределения ППЗК заявками первого класса:

$$\pi_1=\frac{b_1^*}{1-\lambda_1 b_1^*},$$

$$\pi_2=\frac{b_2^*}{(1-\lambda_1 b_1^*)^3},$$

$$\pi_3=\frac{b_3^*}{(1-\lambda_1 b_1^*)^4}+\frac{3\lambda_1(b_2^*)^2}{(1-\lambda_1 b_1^*)^5}.$$

где $b_i^*, i=\overline{1,3}$ — начальные моменты распределения длительности интервала T_{1n}. Поясним способ их нахождения. Согласно [21], ДФР интервалов T_{1n} можно представить формулой

$$\overline{B}_{1n}(t)=[\overline{B}^*(t)]^{n-1}\overline{B}(t),$$

которая имеет прозрачный вероятностный смысл: для одного из каналов, занятого открывшей ППНЗ заявкой берется полное распределение длительности обслуживания, а для прочих — остаточное. Для перехода к начальным моментам используется формула

$$b_m^*=\int_0^\infty t^m dB_{1n}(t)=m\int_0^\infty t^{m-1}\overline{B_{1n}}(t)dt,\ m=\overline{1,l}.$$

В [22–23] приведен способ нахождения данных моментов на основе численного интегрирования по полуоси с весом Чебышева-Лагерра. Итоговая формула для начальных моментов распределения интервала T_{1n} представляет собой

$$b^*{}_m=m\sum_{k=1}^{N}A_k\,\overline{B_{1n}}^*(t_k)e^{t_k},\ m=1,2,...,$$

где A_k и t_k коэффициенты, для которых существуют справочные таблицы для заданного числа N, характеризующего точность вычислений.

Предположим, что ППЗК заявками 1-го класса имеет произвольное распределение, аппроксимируемое одним из распределений фазового типа. Из соображений обеспечения приемлемых характеристик точности и трудоемкости воспользуемся для этого гиперэкспоненциальным распределением второго порядка с параметрами $\{y_i,\eta_i\}, i=\overline{1,2}$.

Теперь для расчета стационарных вероятностей состояний исследуемой СМО можно воспользоваться численными методами итерационного типа [16–20].

Итерационный метод для модели $M^{[2]}/H_2^{[2]}/n/\infty/f_a$

Состояние системы $M^{[2]}/H_2^{[2]}/n/\infty/f_a$ определим кортежем $<j_2;j_1;m^1;m^2;\varphi>$, $j_1=\overline{0,n-1}$, $m^1=<m_1^1,m_2^1>$, $m^2=<m_1^2,m_2^2>$. Здесь j_2 — число заявок 2-го класса в системе; m_i^1 — количество заявок 1-го класса, проходящих обслуживание на i-й ветви гиперэкспоненциального распределения в СМО при $j_1=\overline{0,n-1}$; m_i^2 — количество заявок 2-го класса, проходящих обслуживание на i-й ветви гиперэкспоненциального распределения; φ — номер фазы гиперэкспоненциального представления распределения длительности ППЗК заявками 1-го класса, задаваемый при $j_1=n$ (число заявок 1-го класса в системе при этом не фиксируется и может быть произвольным).

Обозначим $p_j=\{p_{j,1},p_{j,2},...,p_{j,k}\}$ векторы-строки вероятностей нахождения СМО в микросостояниях

Для расчета стационарных вероятностей состояний СМО методами [16–20] необходимо построить матрицы условных интенсивностей переходов по прибытию заявок.

На рис. 1–4 изображены диаграммы условных интенсивностей переходов между состояниями СМО типа $M^{[2]}/H_2^{[2]}/n/\infty/f_a$.

Обозначим через S_j множество всех возможных микросостояний обслуживания на j-м ярусе системы. Через σ_j обозначим количество микросостояний в S_j. Каждые два правых микросостояния j-го яруса связаны с переходами в ППНЗ заявками первого класса. В соответствии с диаграммой переходов формируются следующие матрицы интенсивностей инфинитезимальных переходов:

$A_j[\sigma_j\times\sigma_{j+1}]$ — прибытие заявки второго класса,

$B_j[\sigma_j\times\sigma_{j-1}]$ — уход заявки второго класса по обслуживанию,

$C_j[\sigma_j\times\sigma_j]$– прибытие заявки первого класса,

$D_j[\sigma_j\times\sigma_j]$ — ухода из микросостояний яруса j.

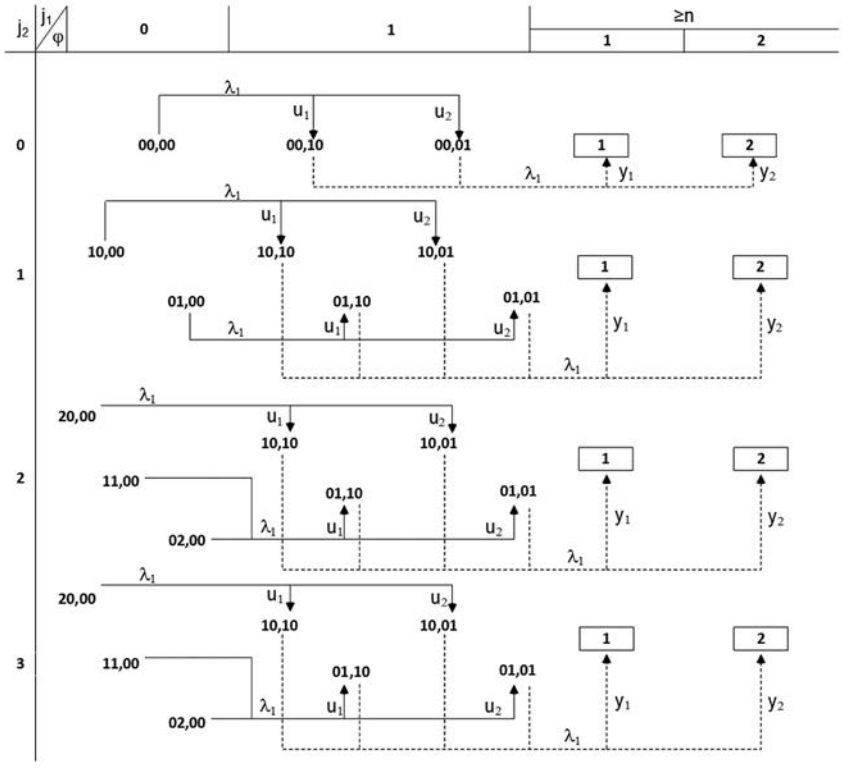


Рис. 1. Переходы при прибытии заявок 1-го класса

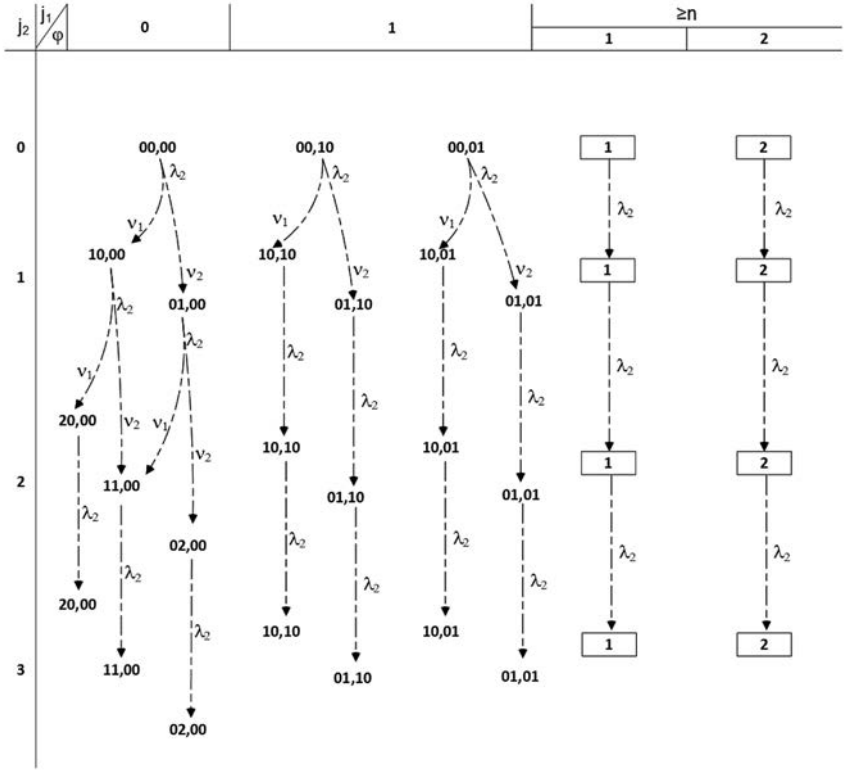


Рис. 2. Переходы при прибытии заявок 2-го класса

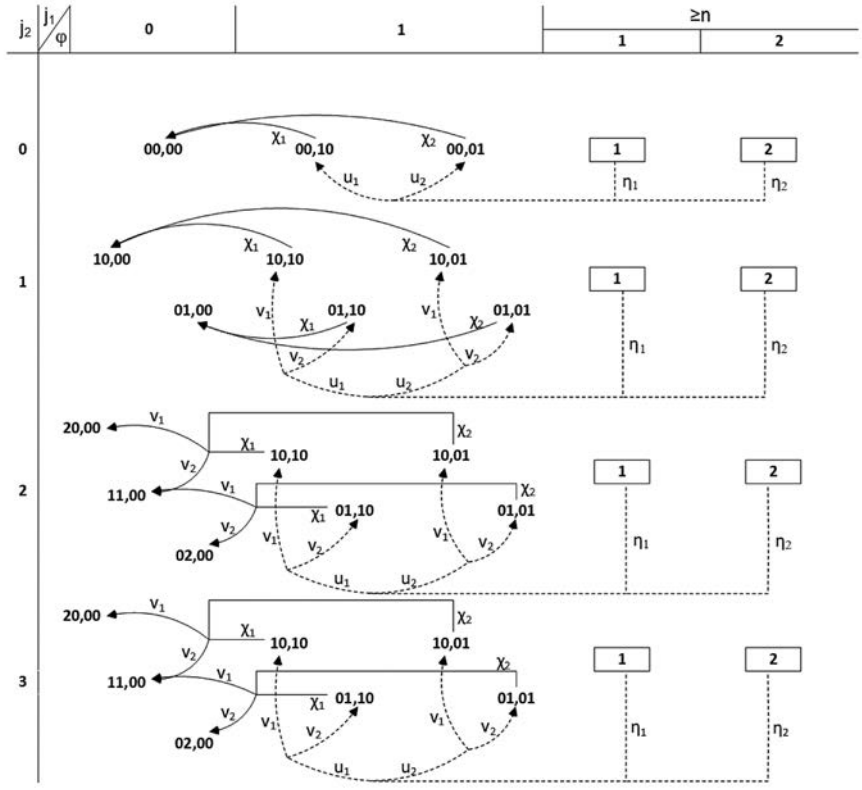


Рис. 3. Переходы по обслуживанию заявок 1-го класса

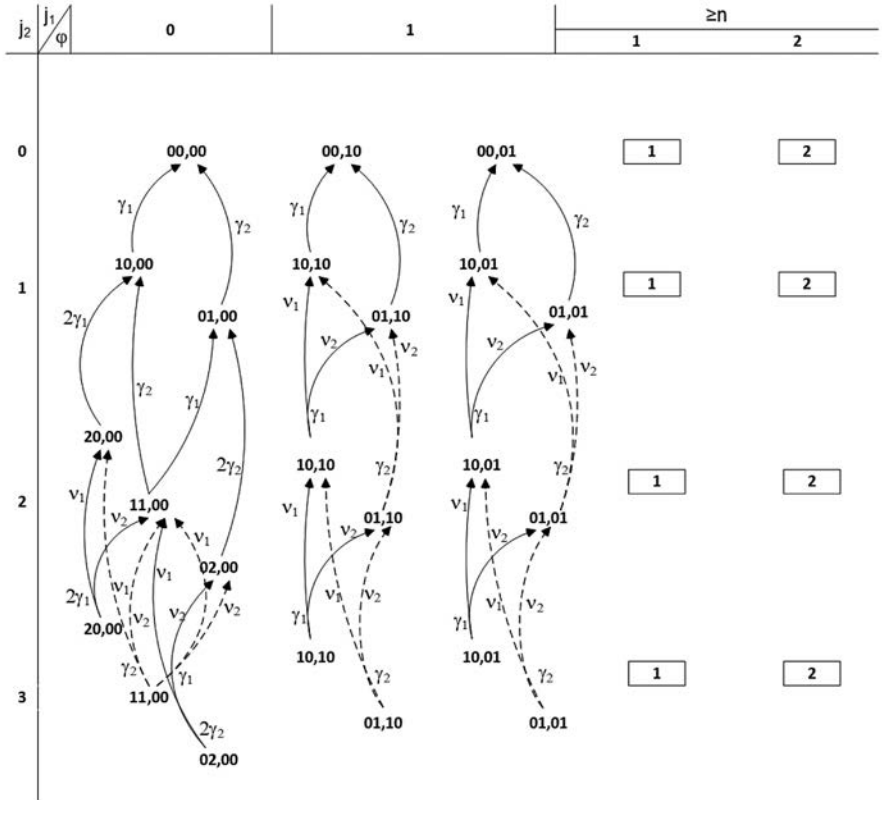


Рис. 4. Переходы по обслуживанию заявок 2-го класса

Введем векторы-строки $\gamma_j = \{\gamma_{j,1}, \gamma_{j,2}, \ldots, \gamma_{j,\sigma_j}\}$ нахождения СМО в состояниях j-го яруса. Запишем векторно-матричные уравнения баланса переходов между состояниями

$$\begin{aligned} &\gamma_0 D_0 = \gamma_0 C_0 + \gamma_1 B_1, \\ &\gamma_j D_j = \gamma_{j-1} A_{j-1} + \gamma_j C_j + \gamma_{j+1} B_{j+1},\ j = 1, 2... \end{aligned} \quad (1)$$

Дальнейший расчет будем производить итерационным методом Такахаси-Таками [20]. Приведем здесь краткое его содержание.

Положим $t_j = \gamma_j / p_j$, где p_j — суммарная вероятность наличия в системе ровно j заявок, и обозначим

$$x_j = p_{j+1} / p_j, \quad z_j = p_{j-1} / p_j.$$

Тогда систему (1) можно переписать относительно векторов условных вероятностей $\{t_j\}$, нормированных к единице в пределах яруса:

$$\begin{aligned} &t_0 D_0 = t_0 C_0 + x_0 t_1 B_1, \\ &t_j D_j = z_j t_{j-1} A_{j-1} + t_j C_j + x_j t_{j+1} B_{j+1} \quad j = 1, 2... \end{aligned}$$

Векторы $t_j^{(m)}$ находятся согласно

$$t_j^{(m)} = z_j^{(m)} \beta'_j + x_j^{(m)} \beta''_j.$$

Здесь

$$\begin{aligned} \beta'_j &= t_{j-1,}^{(m)} A_{j-1} (D_j - C_j)^{-1}, \\ \beta''_j &= t_{j+1,}^{(m-1)} B_{j+1} (D_j - C_j)^{-1}. \end{aligned}$$

При $j = N$ считается, что

$$\beta''_N = t_{N-1,}^{(m)} B_N (D_N - C_N)^{-1}.$$

Расчет $z_j^{(m)}$ происходит согласно формулы

$$z_j^{(m)} = c x_j^{(m)},$$

с коэффициентом

$$c = \frac{\beta''_j B_j 1_{j-1}}{t_{j-1}^{(m)} A_{j-1} 1_j - \beta'_j B_j 1_{j-1}}.$$

В этой и последующих формулах произведения матриц переходов на вектор $\mathbf{1}_j$ равны суммам строк соответствующих матриц и могут быть вычислены однократно до начала итераций. Расчет $x_j^{(m)}$ осуществляется согласно

$$x_j^{(m)} = 1 / (A\beta'_j + \beta''_j) 1_j.$$

Удобным критерием прекращения итераций является условие

$$\max_j \left| x_j^{(m)} - x_j^{(m-1)} \right| \le \varepsilon.$$

Практические расчёты свидетельствует о достаточности $\varepsilon = 10^{-6}$. После прекращения итераций можно переходить к нахождению абсолютных значений вероятностей. Из определения чисел $\{x_j\}$ следуют равенства

$$p_{j+1} = p_j x_j, \quad j = \overline{0, N-1}. \quad (2)$$

Далее принимается p_0=1, а последующие вероятности считаются согласно (2) с одновременным накоплением суммы. Затем, для соблюдения условия нормировки, все вычисленные вероятности делятся на упомянутую сумму.

Результаты расчетов

Предложенный метод реализован с использованием языка программирования C#. На рис. 5 представлены графики распределения вероятностей нахождения в СМО заявок второго класса, полученные в результате численных расчетов и имитационного моделирования (ИМ) для количества каналов $n = 2$ и $n = 3$. Коэффициент загрузки выбирался равным $\rho = 0.85$, на уровне типичных значений для систем с приоритетными дисциплинами обслуживания.

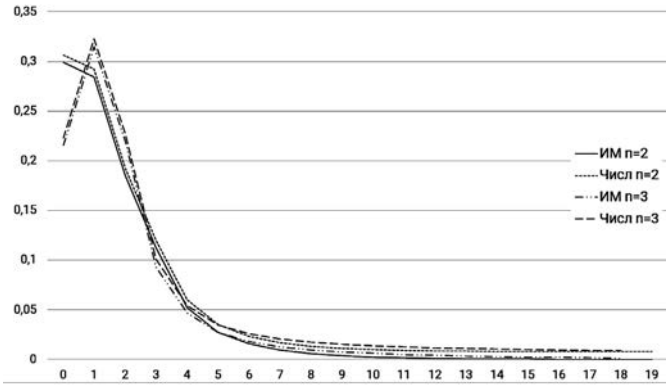


Рис. 5. Стационарное распределение числа заявок 2-го класса

Как видно из рис. 5, наблюдается приемлемое согласие результатов ИМ и численных расчетов.

Заключение

Предложенный метод расчета позволяет найти стационарное распределение вероятностей для СМО с абсолютным приоритетом и произвольным распределением времени обслуживания заявок каждого классов, представленным одним из распределений фазового типа. Показано

приемлемое по точности согласие результатов расчетов с имитационным моделированием.

Направлением дальнейших исследований представляется разработка метода расчета временных характеристик для рассмотренного типа многоканальных СМО с абсолютным приоритетом, а также применения моделей многоканальных приоритетных СМО для решения актуальных современных прикладных задач, например [24].

Литература

1. *Бронштейн О. И., Духовный И. М.* Модели приоритетного обслуживания в информационно-вычислительных системах. М.: Наука, 1976. 220 с.

2. *Климов Г. П.* Стохастические системы обслуживания. М.: Наука, 1966. 276 с.

3. *Конвей Р. В., Максвелл В. Л., Миллер Л. В.* Теория расписаний: пер. с англ. М.: *Наука*, 1975. 359 с.

4. *Гнеденко Б. В., Даниелян Э. А., Димитров Б. Н.* Приоритетные системы обслуживания. М.: Изд-во МГУ, 1973. 447 с.

5. *Buzen J., Bondi A.* Response times of priority classes under preemptive resume in M/M/m queues // Operations Research. 1983. Vol. 31(3). Pp. 456–465.

6. *Kella O., Yechiali U.* Waiting times in the non-preemptive priority M/M/c queue // Stochastic Models. 1985. Vol. 1(2). Pp. 257–262.

7. *Sleptchenko A., van Harten, van der Heijden M. C.* An Exact Solution for the State Probabilities of the Multi-Cass, Multi-Server Queue with Preemptive Priorities // Queueing systems. 2005. Vol. 1. Pp. 81–108.

8. *Zeltyn S., Feldman Z., Wasserfrug S.* Waining and sojourn times in a multi-server queue with mixed priorities // Queueing Systems. 2009. Vol. 61(4). Pp. 305–328.

9. *Altinkemer K., Bose I., Pal R.* Average waiting time of customers in an M/D/k queue with nonpreemptive ptiorities // Computers & Operations Research. 1998. Vol. 25(4). Pp. 317–328.

10. *Harchol-Balter M., Osogami T., Schelter-Wolf A., Wierman A.* Multi-server queueing systems with multiple priority classes // Queueing Systems. 2005. Vol. 51(3). Pp. 331–360.

11. *Wagner D.* Analysis of mean values of a multi-server model with non-preemptive priorities and non-renewal input // Stochastic Models. 1997. Vol. 13(1). Pp. 67–84.

12. *Williams T.* Nonpreemptive multi-server priority queues // Journal of the Operational Research Society. 1980. Vol. 31. Issue 12. Pp. 1105–1107.

13. *Jagerman D. L., Melamed B.* Models and approximations for call center design // Methodology and Computing in Applied Probability. 2003. Vol. 5(2). Pp. 159–181.

14. *HanbaliA. Al., deHaanR., BoucherieR., OmmerenJ.-K.* Time-limited polling systems with batch arrivals and phase-type service times // Annals of Operations Research. 2012. Vol. 198. Issue 1. Pp. 57–82.

15. *Рыжиков Ю. И., Хомоненко А. Д.* Расчет многоканальных систем обслуживания с абсолютным и относительным приоритетами на основе инвариантов отношения // Интеллектуальные технологии на транспорте. 2015. № 3. С. 11–16.

16. *Хомоненко А. Д.* Вероятностный анализ приоритетного обслуживания с прерываниями в многопроцессорных системах // Автоматика и вычислительная техника. 1990. № 2. С. 55–61.

17. *Хомоненко А. Д.* Анализ производительности многопроцессорных систем при приоритетном обслуживании неоднородных потоков запросов // Автоматика и вычислительная техника. 1991. № 4. С. 55–64.

18. *Рыжиков Ю.* И. Алгоритмический подход к задачам массового обслуживания. Монография. СПб.: Изд-во ВКА им. А. Ф. Можайского. 2013. 496 с.

19. *Рыжиков Ю. И., Хомоненко А. Д.* Итеративный метод расчета многоканальных систем с произвольным распределением времени обслуживания // Проблемы управления и теория информации. 1980. № 3. С. 32–38.

20. *Takahashi Y., Takami Y. A* numerical method for the steady-state probabilities of a GI/G/c queuing system in a general class // J. of the Operat. res. soc. of Japan. 1976. Vol. 19(2). Pp. 147–157.

21. *Саати Т. Л.* Элементы теории массового обслуживания и ее приложения: пер. с англ. М.: Сов. радио, 1965. 510 с.

22. *Рыжиков Ю. И., Лохвицкий В. А., Хабаров Р. С.* Метод расчета длительности обработки задач в системе массового обслуживания с учетом процессов Split-Join // Известия высших учебных заведений. Приборостроение. 2019. Т. 62. № 5. С. 419–423.

23. *Хабаров Р. С., Лохвицкий В. А.* Модель оценивания оперативности многопоточной обработки задач в распределенной вычислительной среде с учетом процессов Split-Join // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». 2019. № 1. С. 26–34.

24. *Заяц О. И., Кореневская М. М., Ильяшенко А. С., Мулюха В. А.* Управление пакетными коммутациями в телематических устройствах с ограниченным буфером и повторными заявками с помощью вероятностного выталкивающего механизма и приоритетного обслуживания первичных заявок // Интеллектуальные технологии на транспорте. 2016. № 3 (7). С. 21–30.

CALCULATION OF PREEMPTIVE MULTI-SERVER QUEUEING SYSTEMS WITH HYPEREXPONENTIAL DISTRIBUTIONS OF SERVICE TIMES AND BUSY PERIOD

ROMAN S. KHABAROV,
St-Petersburg, Russia, xabarov1985@gmail.com

ANATOLY D. KHOMONENKO,
St-Petersburg, Russia, khomon@mail.ru

KEYWORDS: queuing theory; multi-server queuing systems; priority queues; preemptive priority; busy period.

ABSTRACT

A numerical method for calculating the stationary distribution of the number of requests for multichannel queuing systems with preemptive priority is proposed. Method is based on approximation of the higher priorities classes stream busy period by the hyperexponential distribution. For reasons of ensuring acceptable accuracy and labor-intensive characteristics, it is assumed that the service time of requests of each class is also represented by a hyperexponential distribution with given parameters. With this approach, the calculation of a system with many classes is carried out by sequential calculation of systems with two classes –a combined stream of requests as the first class requests, and the studied, represented by the second. The number of requests in the queue and for service is fixed only for the second class. A method is proposed for finding the initial moments of the first-class requests busy period on the basis of the interval from the moment the channels are fully occupied by first-class requests until the first service of one of the request completion and numerical integration along the half-axis with the Chebyshev-Laguerre weight. An example of diagrams of conditional intensities of transitions between the states of the system upon arrival and service for each of the classes of requests for a 2-channel queuing system is presented. A method for calculating a system based on the Takahashi-Takami iterative method is shown. Since the efficiency of first-class requests passing does not depend on the lower priority classes requests passage, for calculating the stationary distribution of first-class requests number in multichannel systems with hyperexponential distribution of servicing without priorities iterative type numerical methods are used. The method is implemented in the high-level programming language C #, an example of calculating the stationary distribution of the number of requests for a 2-channel and 3-channel queuing system, presented using the proposed method and a simulation model, is presented. A fairly high degree of consistency was obtained.

REFERENCES

1. Bronshtejn O.I., Duhovnyj I.M. *Modeli prioritetnogo obsluzhivaniya v informacionno-vychislitel'nyh sistemah* [Priority Service Models in Computer Systems]. Moscow: Nauka, 1976. 220 p. (In Russian)

2. Klimov G.P. *Stohasticheskie sistemy obsluzhivaniya* [Stochastic Service Systems] Moscow: Nauka, 1966. 276 p. (In Russian)

3. Conway R.W., Maxwell W.L., Miller L.W. Theory of Scheduling. Boston: Addison-wesley, 1967. 304 p.

4. Gnedenko B.V., Danielyan E.A., Dimitrov B.N. *Prioritetnye sistemy obsluzhivaniya* [Priority Service Systems]. Moscow: Lomonosov Moscow State University Publ., 1973. 447 p. (In Russian)

5. Buzen J., Bondi A. Response times of priority classes under preemptive resume in M/M/m queues. *Operations Research*. 1983. Vol. 31(3). Pp. 456–465.

6. Kella O., Yechiali U. Waiting times in the non-preemptive priority M/M/c queue. *Stochastic Models*. 1985. Vol. 1(2). Pp. 257–262.

7. Sleptchenko A., van Harten, van der Heijden M.C. An Exact Solution for the State Probabilities of the Multi-Cass, Multi-Server Queue with Preemptive Priorities. *Queueing systems*. 2005. Vol. 1. Pp. 81–108.

8. Zeltyn S., Feldman Z., Wasserfrug S. Waining and sojourn times in a multi-server queue with mixed priorities. *Queueing Systems*. 2009. Vol. 61(4). Pp. 305–328.

9. Altinkemer K., Bose I., Pal R. Average waiting time of customers in an M/D/k queue with nonpreemptive ptiorities. *Computers & Operations Research*. 1998. Vol. 25(4). Pp. 317–328.

10. Harchol-Balter M., Osogami T., Schelter-Wolf A., Wierman A. Multi-server queueing systems with multiple priority classes. *Queueing Systems*. 2005. Vol. 51(3). Pp. 331–360.

11. Wagner D. Analysis of mean values of a multi-server model with non-preemptive priorities and non-renewal input. *Stochastic Models*. 1997. Vol. 13(1). Pp. 67–84.

12. Williams T. Nonpreemptive multi-server priority queues. *Journal of the Operational Research Society*. 1980. Vol. 31. Issue 12. Pp. 1105–1107.

13. Jagerman D.L., Melamed B. Models and approximations for call center design. *Methodology and Computing in Applied Probability*. 2003. Vol. 5(2). Pp. 159–181.

14. Hanbali A. Al., de Haan R., Boucherie R., Ommeren J.-K. Time-limited polling systems with batch arrivals and phase-type service times. *Annals of Operations Research*. 2012. Vol. 198. Issue 1. Pp. 57–82.

15. Ryzhikov Yu.I., Calculation of Multi-Channel Queueing Systems

with Absolute and Relative Priorities on the Basis of Invariants Relationship. *Intellectual Technologies on Transport*. 2015. No. 3. Pp. 11–16. (In Russian)

16. Khomonenko A.D. Probabilistic priority service analysis with interruptions in multiprocessor systems. *Automatic Control and Computer Sciences*. 1990. No. 2. Pp. 55–61. (In Russian)

17. Khomonenko A.D. Performance analysis of multiprocessor systems in the priority service of heterogeneous request streams. *Automatic Control and Computer Sciences*. 1991. No. 25 (4). Pp. 53–61. (In Russian)

18. Ryzhikov Y.I. *Algoritmicheskij podhod k zadacham massovogo obsluzhivaniya* [Algorithmic approach to queuing problems: Monograph]. St. Petersburg: Mozhaisky Military Space Academy Publ., 2013. 496 p. (In Russian)

19. Ryzhikov Yu.I., Khomonenko A.D. Iterativnyj metod rascheta mnogokanal'nyh sistem s proizvol'nym raspredeleniem vremeni obsluzhivaniya [An iterative method for calculating multichannel systems with an arbitrary distribution of service time] *Problemy upravleniya i teoriya informacii* [Management Issues and Information Theory]. 1980. No. 3. Pp. 32–38. (In Russian)

20. Takahashi Y., Takami Y. A numerical method for the steady-state probabilities of a GI/G/c queuing system in a general class. *J. of the Operat. res. soc. of Japan*. 1976. Vol. 19(2). Pp. 147–157.

21. Saaty T.L. *Elements of queueing theory, with applications*. New York: McGraw-Hill, 1961. 436 p.

22. Ryzhikov Y.I., Lohvickij V.A., Khabarov R.S. Method of calculating task treatment duration in queueing system with consideration of Split-Join processes. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [Journal of Instrument Engineering]. 2019. Vol. 62. No. 5. Pp. 419–423. (In Russian)

23. Khabarov R.S., Lohvickij V.A. Efficiency evaluation model of parallel processing in distributed environment using Split-Join queue. *Vestnik of Russian New University. Series: Complex systems: models, analysis, management*. 2019. No. 1. Pp. 26–34. (In Russian)

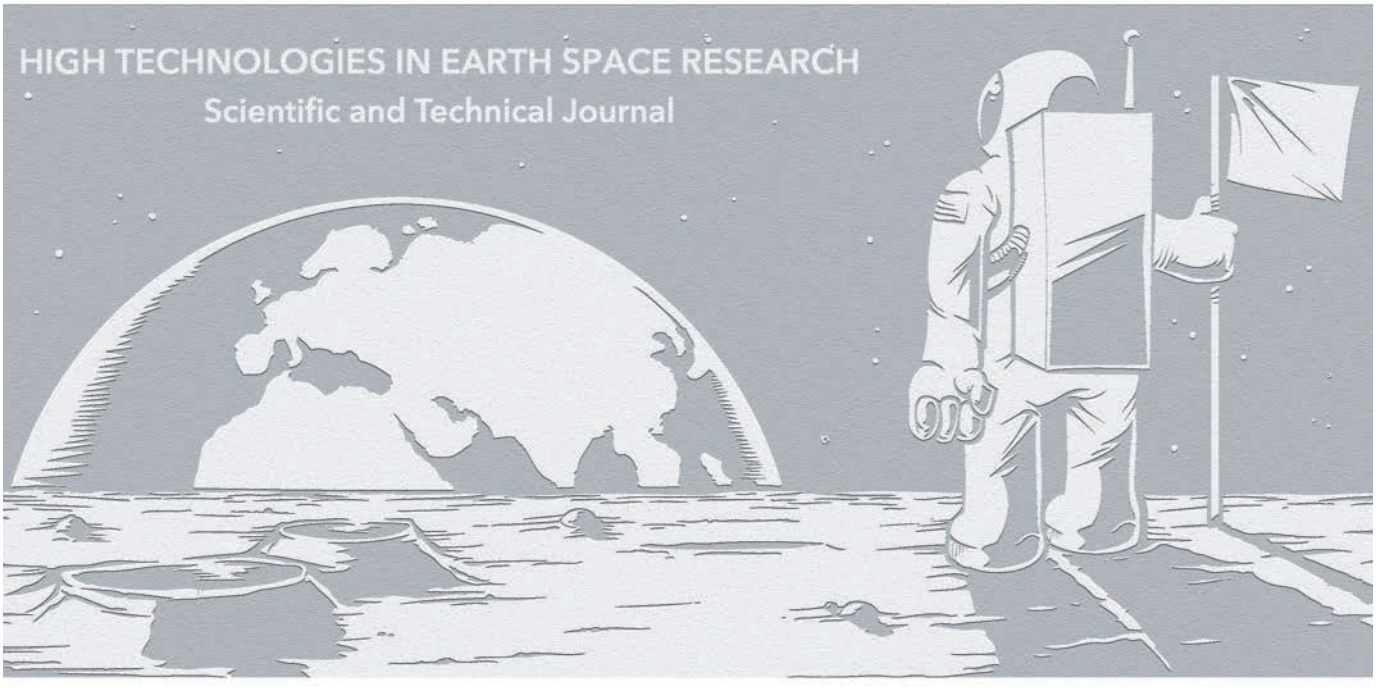
24. Zayats O.I., Korenevskaya M.M., Ilyashenko A.S., Muliukha V.A. Network Packets Management in Telematic Devices with Retrial, Limited Buffer Size Using Randomized Push-Out Mechanism and Prioritization for Initial Flow. *Intellectual Technologies on Transport*. 2016. No. 3 (7). Pp. 21–30. (In Russian)

INFORMATION ABOUT AUTHORS:

Khabarov R.S., Postgraduate at the Department of the Military Space Academy;

Khomonenko A.D., PhD, Professor, Head of Department of Emperor Alexander I Petersburg State Transport University, Professor at the Department of the Military Space Academy.

For citation: Khabarov R.S., Khomonenko A.D. Calculation of preemptive multi-server queueing systems with hyperexponential distributions of service times and busy period. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 48–56. doi: 10.24411/2409-5419-2018-10287 (In Russian)



doi: 10.24411/2409-5419-2018-10288

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К СОВЕРШЕНСТВОВАНИЮ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ НА ОСНОВЕ ПРИМЕНЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

ЯМПОЛЬСКИЙ
Сергей Михайлович

АННОТАЦИЯ

Опыт проведения мероприятий оперативной подготовки показал, что эффективность управления войсками (силами) во многом зависит от оперативности расчетов, обоснованности и достоверности результатов прогнозирования основных показателей управления, а также от наглядности полученных результатов. В связи с этим, представляется целесообразным внедрение в деятельность органов военного управления интеллектуальных систем, основу которых будут составлять многофункциональные моделирующие комплексы, адекватно отражающие реальные условия протекания операций (боевых действий), учитывающие закономерности и взаимные связи между ними. В работе рассмотрены особенности автоматизации деятельности органов военного управления и проблемы, препятствующие внедрению интеллектуальных систем, а также представлена структура интеллектуальной системы и предложена схема ее применения в ходе информационно-аналитической поддержки деятельности органов военного управления. В качестве примера рассмотрено возможное применение интеллектуальной системы при автоматизированной разработке системы планирующих, директивных, отчетно-информационных и справочных документов, формируемых должностными лицами органов военного управления в ходе решения поставленных задач. В заключение сформулированы рекомендации по совершенствованию деятельности органов военного управления.

Сведения об авторе:

к.т.н., доцент, старший научный сотрудник Военного института (управления национальной обороной) Военной академии Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия, yampolsm@mail.ru

КЛЮЧЕВЫЕ СЛОВА: органы военного управления; управление войсками; боевые действия; интеллектуальная система; автоматизированная система; комплекс программных средств; база данных; база знаний; система документов.

Для цитирования: *Ямпольский С.М.* Концептуальный подход к совершенствованию деятельности органов военного управления на основе применения интеллектуальных систем // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 57–64. doi: 10.24411/2409-5419-2018-10288

Введение

Необходимость внедрения интеллектуальных систем в различные сферы деятельности общества была подробно обоснована в программе «Цифровая экономика Российской Федерации», сформированной на основе «Стратегии развития информационного общества в Российской Федерации» на 2017–2030 годы и утвержденной Распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632.

Основной целью принятия данной программы является формирование информационного пространства с учетом развития инфраструктуры Российской Федерации, создание и применение российских информационно-телекоммуникационных систем, а также формирование новой информационно-технологической основы для социальной и экономической сферы [1–2].

Необходимость приложения основных положений этой программы для повышения эффективности *деятельности органов военного управления* была обоснована в ряде научных работ [3–6] в которых подчеркивалось, что применение интеллектуальных систем в интересах совершенствования деятельности органов управления позволит:

выделять наиболее значимые данные обстановки;

выполнять очистку (фильтрацию) данных обстановки на основе заданной классификации в целях повышения их качества и достоверности;

проводить оперативную аналитическую обработку данных обстановки на основе решения типовых расчетно-аналитических задач;

выполнять статистический и динамический информационно-поисковый анализ данных обстановки;

выявлять скрытые закономерности и особенности данных обстановки;

формировать информацию, содержательно интерпретирующую данные обстановки путем их представления в табличном и графическом виде в целях проведения автоматического (автоматизированного) экспертного анализа.

Установлено, что для практического применения интеллектуальных систем нужно учитывать ряд особенностей, связанных с существующим положением дел в области автоматизации деятельности ОВУ, а также большие издержки и риски, которые неизбежно будут сопровождать их реализацию.

Такими особенностями являются:

разнородность — данные измеряются в разных шкалах;

неполнота — имеются пропуски в данных;

неточность — данные измеряются с погрешностями;

противоречивость — разные результаты, получаемые путем наблюдения над одинаковыми объектами;

избыточность — наличие большого объема неиспользуемых статистических данных;

неструктурированность — отсутствие описания многих признаков данных;

качество — наличие нетривиальных критериев качества данных.

В применяемых сегодня ОВУ автоматизированных системах военного назначения (АС ВН) неполнота исходных данных обстановки существенно снижает возможности информационно-аналитической поддержки решений, принимаемых руководящими лицами этих органов управления, либо вообще не позволяет осуществить такую поддержку [6].

Большинство применяемых ОВУ автоматизированных систем в лучшем случае позволяют обобщать данные обстановки о произошедших событиях, оценивать исполнительскую дисциплину должностных лиц или степень достижения ими значений показателей деятельности на основе бинарной оценки «выполнено — не выполнено». При этом управленческие решения, как правило, принимаются только на основе опыта и интуиции руководящих лиц органов управления.

С учетом того, что в ходе ведения операций (боевых действий) схожие ситуации практически отсутствуют, создание алгоритмов, пригодных для всех случаев боевого управления войсками (силами) становится практически невозможным [6]. Следовательно, интеллектуальные системы должны стать ключевыми инструментами, обеспечивающими повышение эффективности деятельности ОВУ.

Результаты проведенных исследований показали, что для успешного применения интеллектуальных систем в деятельности ОВУ необходимо решить ряд проблем, к числу которых относятся:

изучение и формализация различных схем умозаключений должностных лиц ОВУ на основе разнородной информации, используемой в процессе решения поставленных задач;

разработка методов структуризации, классификации и формализации знаний из различных проблемных областей деятельности ОВУ;

создание диалоговых процедур общения на естественном языке, обеспечивающих контакт между интеллектуальной системой и должностными лицами ОВУ в процессе решения поставленных задач;

обучение интеллектуальной системы в процессе ее деятельности, создание алгоритмов накопления и обобщения знаний.

Место интеллектуальной системы в информационно-аналитической поддержке деятельностиорганов военного управления

Анализ задач, решаемых ОВУ, позволяет сделать вывод, что большинство из них являются многокритериальными задачами, для решения которых приходится учитывать большое число факторов, интересов и последствий,

характеризующих варианты принимаемых решений. При этом для процессов деятельности ОВУ характерно вероятностное поведение, связанное с воздействием множества объективных и субъективных факторов (например, связанных с динамично изменяющейся обстановкой). Отсюда вытекает потребность в такой интеллектуальной системе, которая бы взяла на себя все формализованные функции должностных лиц ОВУ и оказала бы им существенную поддержку при решении трудно формализуемых задач. Применение таких систем создаст условия для объединения в единое целое всего многообразия разнородной информации, циркулирующей в ОВУ, к виду, позволяющему представлять обстановку адекватно реальной.

В частности, для повышения эффективности деятельности ОВУ необходимо создание и внедрение интеллектуальной системы, связанной с обеспечением разведывательной информацией, с проведением оценки обстановки, с планированием и управлением операциями (боевыми действиями), с обеспечением взаимодействия и всестороннего обеспечения проводимых операций.

Схема возможного применения интеллектуальной системы в деятельности ОВУ представлена на рис. 1.

В соответствии со схемой, данные текущей обстановки вводятся в фактографическую базу данных, предназначенную для регистрации и хранения данных обстановки, а также данных об используемых объектах предметной области.

В результате, в фактографической базе данных формируются исходные данные для:

работы программного средства «Формирования системы планирующих, директивных, отчетно-информационных и справочных документов»;

проведения расчетов с помощью комплекса программных средств (КПС) управления войсками;

оценки данных обстановки и получения новых знаний с помощью интеллектуальной системы.

Результаты моделирования, выполненные с помощью КПС управления войсками, и результаты решения информационно-расчетных задач заносятся в фактографическую базу данных, поступают для анализа в интеллектуальную систему, а также отображаются на средствах визуализального отображения информации.

Необходимость применения в рассматриваемой схеме интеллектуальной системы обусловлена тем, что использование должностными лицами органов управления только моделей и информационно-расчетных задач является недостаточным для принятия обоснованных управленческих решений. В частности, применение математического моделирования в каждом конкретном случае требует наличия адекватной модели и измеримости исследуемых характеристик, что в реальности встречается достаточно редко [10].

Структура интеллектуальной системы показана на рис. 2. Ее составными частями являются:

средства общения с пользователями, позволяющие осуществлять обмен данными между ними и интеллектуальной системой, путем преобразования поступающих сообщений в форму представления базы знаний, а также

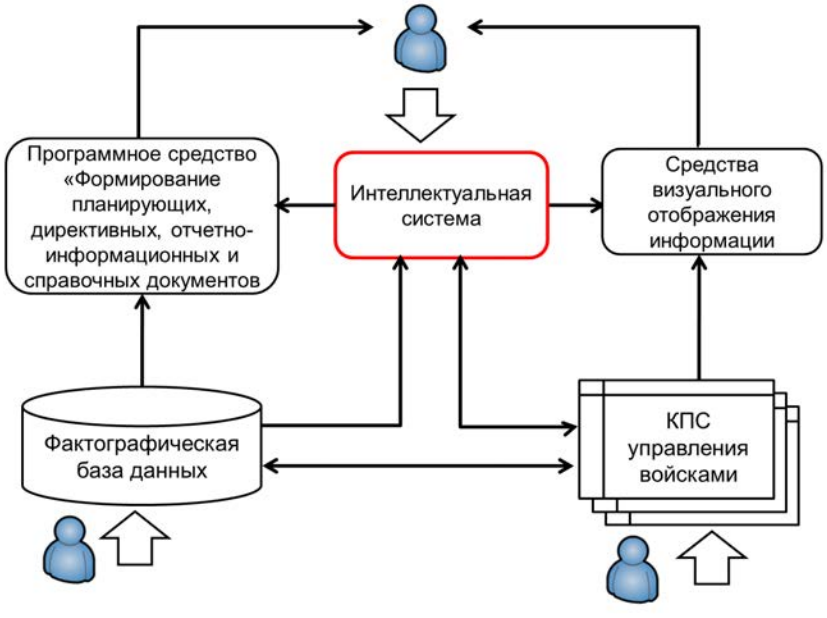


Рис. 1. Схема применения интеллектуальной системы в деятельности ОВУ

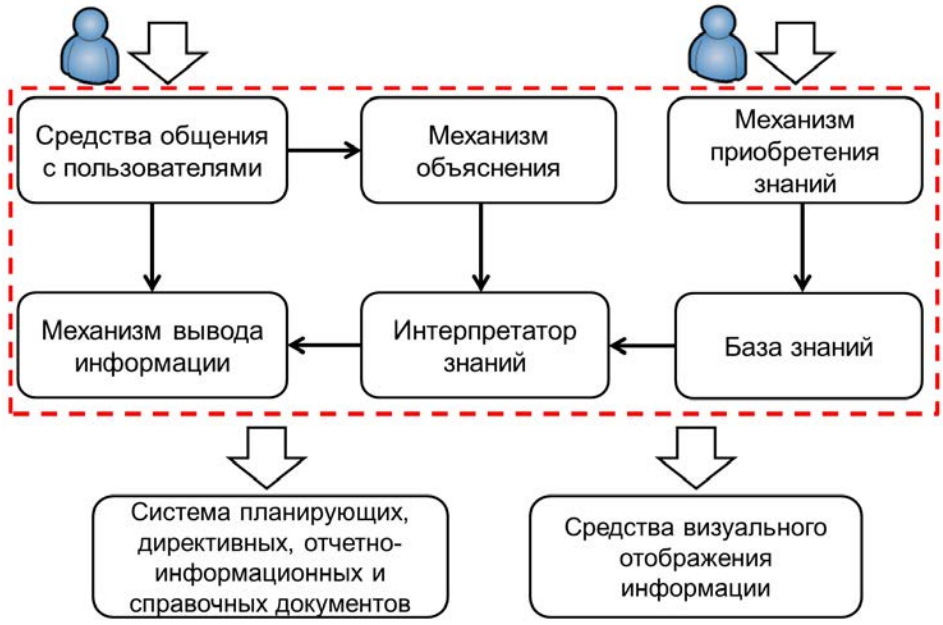


Рис. 2. Структура интеллектуальной системы

переводить внутреннее представление результата обработки сообщения базой знаний в формат, понятный должностным лицам;

механизм вывода информации, позволяющий получать от средств общения с пользователями преобразованный во внутреннее представление запрос, формировать из базы знаний конкретный алгоритм решения задачи, выполнять данный алгоритм, а полученный результат решения предоставлять средствам общения с пользователями для выдачи ответа на поступающие запросы;

механизм объяснения, необходимый для получения обоснованных путей выхода из проблемной ситуации. При этом возможна выдача должностным лицам цепочки рассуждений до требуемой контрольной точки с заранее подготовленными комментариями;

механизм приобретения знаний, необходимый для ввода полученных знаний в базу знаний и их последующего обновления.

Применение интеллектуальной системы позволит, в условиях априорно неполной информации, формировать недостающие исходные данные обстановки и контролировать корректность вводимых данных. Это позволит обрабатывать и выдавать требуемую информацию, а также рассчитывать все варианты последующих действий войск (сил). При этом применение интеллектуальной системы для обработки результатов моделирования позволит прогнозировать действия по выполнению поставленных задач и оценивать их результаты по выбранным показателям и критериям.

Применение в интеллектуальной системе базы знаний позволит накапливать и структурировать информацию о принятых управленческих решениях в различных ситуациях, предлагать варианты управленческих решений, быстро реагировать на изменения текущей обстановки, а также запоминать результаты своих прошлых действий и руководствоваться ими в дальнейшей работе [6]. Целесообразно, чтобы рассматриваемая база знаний объединяла функционал управления знаниями, анализа данных обстановки и интеллектуальной поддержки принятия решений, а ключевым принципом ее работы должно стать накопление знаний, которые могут быть напрямую использованы должностными лицами ОВУ. Это позволит объединить технологии, реализуемые в системах поддержки принятия решений, и технологий онтологического хранения данных. В совокупности эти технологии способны сформировать решение, гибкость которого окажется достаточной для интеллектуального информационного сопровождения деятельности ОВУ.

При создании рассматриваемой интеллектуальной системы целесообразно использовать технологии нейронных сетей, что связано с необходимостью учета исторических особенностей исследуемых процессов. При этом применение классической рекуррентной нейронной сети является нецелесообразным ввиду ее неспособности к управляемому сохранению информации о предыдущих итерациях и высокой скорости замещения памяти нейронной сети.

Предлагается интеллектуальную систему построить на основе нейронной сети с долгой краткосрочной памя-

тью — особой разновидности архитектуры рекуррентных нейронных сетей, способной к обучению долговременным зависимостям.

Применение интеллектуальной системы при разработке системы планирующих, директивных, отчетно-информационных и справочных документов

Рассмотрим применение интеллектуальной системы при автоматизированной разработке системы планирующих, директивных, отчетно-информационных и справочных документов, формируемых должностными лицами ОВУ в ходе решения поставленных задач.

Такая система документов должна быть сформирована на основе данных содержащихся в фактографической базе данных, с поддержкой автоматического наполнения документов актуальными данными обстановки (данными о состоянии войск, местности, объектов и т.д.), а также знаниями, полученными из интеллектуальной системы на основе результатов моделирования и решения информационно-расчетных задач.

В соответствии с правилами организации электронного документооборота, каждый формируемый документ должен включать реквизитную и содержательную части. В связи с этим, для автоматизированного формирования системы документов каждому блоку содержательной части документа также должен быть присвоен уникальный идентификатор, связанный с заданными разделами фактографической базы данных.

В результате будет сформирован формуляр документа — структурированное описание содержательной части документа. При этом одному формуляру может соответствовать несколько шаблонов документов (рис. 3).

После запуска процесса формирования шаблона документа в каждое имеющее у него «поле для ввода» будут автоматически загружены данные из соответствующего формуляра документа и информация из интеллектуальной системы.

Возможный вид шаблона документа «Предварительное боевое распоряжение» представлен на рис. 4.

При заполнении поля шаблона «Постановка задач войскам (силам)» возникает объективная необходимость применения интеллектуальной системы. Это связано с тем, что при сравнении различных вариантов порядка оперативного построения группировки войск (сил) часто требуется принимать решение о предпочтительности того или иного варианта по совокупности количественных и качественных показателей.

Применение интеллектуальной системы позволит сформировать обоснованные весовые коэффициенты для расчета интегральных показателей, характеризующих различные варианты порядка оперативного построения группировки войск (сил), учесть исторические данные об объектах управления, построить корректный прогноз по дальнейшему развитию событий и выполнить свертку исследуемых показателей с учетом рассчитанных интеллектуальной системой весовых коэффициентов.

Например, в рамках проведения расчета боевого потенциала личного состава войск (сил) актуальной задачей является определение коэффициентов их подготовленности и морально-психологического состояния, а также коэффициента важности военно-учетной специальности. Для адекватного расчета этих коэффициентов интеллектуальной системой будут учтены исторические данные, характерные для рассматриваемых процессов, полученные на основе обучения интеллектуальной системы.

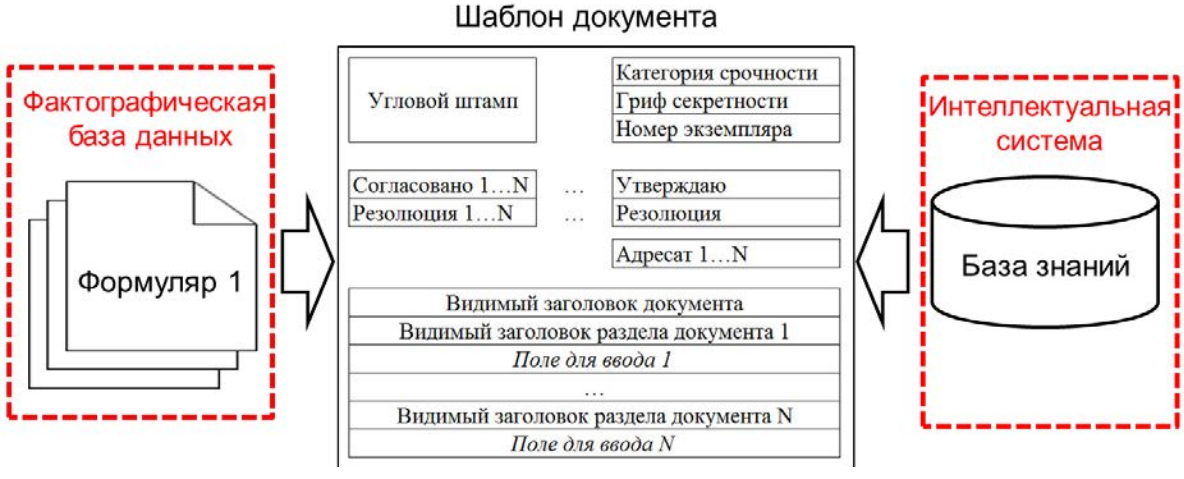


Рис. 3. Представление шаблона документа на основе данных формуляра и информации из интеллектуальной системы

Рис. 4. Возможный вид шаблона документа

Заключение

На основе изложенного материала сформулируем рекомендации ОВУ, выполнение которых актуально при совершенствовании деятельности этих органов управления.

К таким рекомендациям относятся:

– внедрение новых технических решений, реализуемых на основе территориально-распределенной обработки данных, с использованием «облачных технологий», которые обеспечат формирование виртуального пространства военных действий любого масштаба;

– обеспечение перехода от документального к фактографическому обмену данными в интересах повышения оперативности управления (в первую очередь процесса разработки документов) в реальном масштабе времени с широким использованием интеллектуальных систем, ориентированных на непрерывный мониторинг обстановки;

– реализация комплексной автоматизации всего информационно-вычислительного процесса информационной поддержки деятельности ОВУ взаимоувязанными компонентами программного, информационного и лингвистического обеспечения;

– проведение работ по дальнейшему совершенствованию и модернизации АС ВН с целью внедрения интеллектуальных технологий;

– уточнение состава информации, подлежащей обмену между ОВУ и синхронизация деятельность участников информационного взаимодействия;

– организация профессиональной подготовки должностных лиц ОВУ по вопросам применения интеллектуальной системы с привлечением специалистов промышленности.

Таким образом, внедрение интеллектуальных систем в деятельность ОВУ обеспечит возможность детального учета различных по природе факторов, объектов, их связей, правил поведения. Это позволит получать результаты, характерные для рассматриваемой деятельности, которые прежние методы и средства информационной поддержки обеспечить не могли. В частности, применение интеллектуальной системы позволит формировать недостающие исходные данные обстановки, обрабатывать и выдавать требуемую информацию, а также рассчитывать все варианты последующих действий должностных лиц. При этом появится возможность изменить многие организационные формы процесса управления, например, отказаться от такого понятия, как периодичность в прохождении документов, а также повысить степень автоматизации контроля управляемых процессов и качество управления.

Представленный концептуальный подход не означают, что все управленческие решения в области военного управления должны приниматься исключительно с помощью интеллектуальных систем, а обязанности должностных лиц органов управления должны выполнять роботы.

Внедрение интеллектуальных систем в деятельность ОВУ действительно подразумевает передачу им некоторых функций должностных лиц. При этом функционал этих систем не призван заменить должностных лиц, а предназначен для упрощения их деятельности, повышая тем самым её суммарную эффективность.

В завершении статьи необходимо отметить, что практическое применение интеллектуальных систем в деятельности ОВУ связано с необходимостью преодоления многочисленных препятствий, к числу которых относятся:

– отсутствие у должностных лиц ОВУ, воспитанных на традиционных технологиях и методах труда, глубокого понимания необходимости внедрения интеллектуальных систем;

– отсутствие единства взглядов на создание интеллектуальных систем у должностных лиц органов управления;

– недостаток специалистов, профессионально подготовленных к внедрению и применению интеллектуальных систем.

Для преодоления этих препятствий необходима совместная, скоординированная деятельность всех должностных лиц ОВУ.

Литература

1. Программа «Цифровая экономика Российской Федерации», утвержденная Распоряжением Правительства Российской Федерации от 28.07.2017 г. № 1632-р // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения 5.02.2019).

2. Об утверждении программы «Цифровая экономика Российской Федерации». 2018. URL: http://government.ru/docs/28653 (дата обращения 5.02.2019).

3. *Буренок В. М., Дурнев Р. А., Крюков К. Ю.* Разумное вооружение: будущее искусственного интеллекта в военном деле // Вооружение и экономика. 2018. № 1 (43). С. 45–54.

4. *Ямпольский С. М., Анисимов Е. Г.* Концептуальные и методологические основы создания систем информационно-аналитического обеспечения деятельности органов военного управления: монография. М.: Изд-во ВАГШ ВС РФ, 2018. 152 с.

5. *Ямпольский С. М., Анисимов Е. Г., Анисимов В. Г.* Научно-методические основы информационно-аналитического обеспечения деятельности органов государственного и военного управления в ходе межведомственного информационного взаимодействия: монография. М.: Изд-во ВАГШ ВС РФ, 2019. 146 с.

6. *Буренок В. М.* Применение искусственного интеллекта в военном деле // Арсенал отечества. 2018. № 1 (33). С. 18–22.

7. *Добролюбова Е. И., Юшаков В. Н., Ефремов Л. А., Клочкова Е. Н. Талапина Э. В., Старцев Я. Ю.* Цифровое будущее государственного управления по результатам. М.: Дело, 2019. 114 с.

8. *Тельнов Ю. Ф.* Интеллектуальные информационные системы. М.: Бином, 2004. 82 с.

9. *Ямпольский С. М., Кузин В. А., Шаламов А. С., Рубинов В. И.* Актуальные вопросы информационно-аналитического обеспечения органов военного управления // Материалы IV Всероссийской научно-практической конференции «Академические Жуковские чтения» (Воронеж, 22–23 ноября 2017 г.). Воронеж, 2017. С. 206–211.

10. *Рудаков К. В.* Некоторые вопросы применения современных методов интеллектуального анализа больших табличных и текстовых данных // Материалы II межведомственной научно-практической конференции «Система межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации» (Москва, 25 ноября 2016 г.). Москва, 2016. С. 96–99.

11. *Кравченко Т. К., Исаев Д. В.* Системы поддержки принятия решений. М.: Юрайт, 2016. 292 с.

12. *Рыбина Г. В.* Основы построения интеллектуальных систем. М.: Финансы и статистика, 2014. 432 с.

CONCEPTUAL APPROACH TO THE IMPROVEMENT OF MILITARY MANAGEMENT BODIES FUNCTIONING BASED ON THE USE OF INTELLIGENT SYSTEMS

SERGEY M. YAMPOLSKY,
Moscow, Russia, yampolsm@mail.ru

KEYWORDS: military management bodies; forces management; combat actions; intelligent system; automated system; software complex; database; knowledge base; document system.

ABSTRACT

The experience of conducting operational preparations has proven that the efficiency of forces management depends a lot on the promptness of the computations, feasibility and legitimacy of the main control indicator prognosis, and on the illustrativeness of obtained result. In that regard, it is reasonable to incorporate intelligent systems based on multifunctional modelling complexes, which adequately depict real conditions of combat actions course and also considers patterns and mutual links between them, into military management bodies functioning. This work addresses the particularities of military management bodies functioning automation and problems which prevent the application of an intelligent system, and the article also contains the structure of an intelligent system and offers the scheme

of its application for informational and analytical maintenance for the activities of military management bodies. The possible application of an intelligent system for automated development of the system of scheduling, prescriptive, reporting-informational and manual documents formed by the officials of military management bodies in the process of accomplishment of set objectives is considered.

REFERENCES

1. Programma «Cifrovaja jekonomika Rossijskoj Federacii» № 1632-r. [Program "Digital economics of the Russian Federation", approved by the order of the Russian Federation Government (28.07.2017, № 1632-p.)]. *Konsul'tantPlyus*. URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (date of access 5.02.2019). (In Russian)
2. Ob utverzhdenii programmy "Cifrovaja jekonomika Rossijskoj Federacii" [About the approval of the program "Digital economics of the Russian Federation"]. 2018. URL: http://government.ru/docs/28653 (date of access 05.02.2019). (In Russian)
3. Burenok V.M., Durnev R.A., Krukov K.U. Reasonable arming: the future of artificial intelligence in military forces. *Vooruzhenie i jekonomika* [Arming and economics]. 2018. No. 1(43). Pp. 45–54. (In Russian)
4. Jampol'skij S.M., Anisimov E.G. *Konceptual'nye i metodologicheskie osnovy sozdanija sistem informacionno-analiticheskogo obespechenija dejatel'nosti organov voennogo upravlenija* [Conceptual and methodological basics of the implementation of systems of informational and analytical maintenance for the activities of military management bodies]. Moscow: VAGSH VS RF Publ., 2018. 152 p. (In Russian)
5. Jampol'skij S.M., Anisimov E.G., Anisimov V.G. *Nauchno-metodicheskie osnovy informacionno – analiticheskogo obespechenija dejatel'nosti organov gosudarstvennogo i voennogo upravlenija v hode mezhvedomstvennogo informacionnogo vzaimodejstvija* [Scientific and methodological basics of the implementation of systems of informational and analytical maintenance for the activities of military management bodies and public administration during interagency informational interaction]. Moscow: VAGSh VS RF Publ., 2019. 146 p. (In Russian)
6. Burenok V.M. Use of artificial intelligence in military forces. *Arsenal otechestva* [The arsenal of homeland]. 2018. No. 1(33). Pp.18–22. (In Russian)
7. Dobroljubova E.I., Jushakov V.N., Efremov L.A., Klochkova E.N. Talapina Je.V., Starcev Ja. Ju. *Cifrovoe budushhee gosudarstvennogo upravlenija po rezul'tatam* [Digital future of the public administration based on the results]. Moscow: Delo, 2019. 114 p. (In Russian)
8. Tel'nov Ju.F. *Intellektual'nye informacionnye sistemy.* [Intelligent informational systems]. Moscow: Binom, 2004. 82 p. (In Russian)
9. Jampol'skij S.M., Kuzin V.A., Shalamov A.S., Rubinov V.I. Aktual'nye voprosy informacionno-analiticheskogo obespechenija organov voennogo upravlenija [Actual questions of informational and analytical maintenance of military management bodies]. *Materialy IV Vserossijskoj nauchno-prakticheskoj konferencii "Akademicheskie Zhukovskie chtenija"* [Materials of the IV Russian scientific and practical conference научно-практической "Academic Zhukov readi ngs", Voronezh, 22–23 November 2017]. Voronezh, 2017. Pp. 206–211. (In Russian).
10. Rudakov K.V. Nekotorye voprosy primenenija sovremennyh metodov intellektual'nogo analiza bol'shih tablichnyh i tekstovyh dannyh [Several questions of application of modern methods of intellectual analysis of big tabular and text data]. *Materialy II mezhvedomstvennoj nauchno-prakticheskoj konferencii "Sistema mezhvedomstvennogo informacionnogo vzaimodejstvija pri reshenii zadach v oblasti oborony Rossijskoj Federacii"* [Materials of the II interagency scientific and practical conference "The system of interagency informational interaction while solving tasks on the defense of the Russian Federation", Moscow, 25 November 2016)]. Moscow. Pp. 96–99. (In Russian)
11. Kravchenko T.K., Isaev D.V. *Sistemy podderzhki prinjatija reshenij* [Decision Support Systems]. Moscow: Jurajt, 2016. 292 p. (In Russian)
12. Rybina G.V. *Osnovy postroenija intellektual'nyh system* [The basics of intelligent system construction]. Moscow: Finansy i statistika, 2014. 432 p. (In Russian)

INFORMATION ABOUT AUTHOR:

Yampolsky S.M., Candidate of technical Sciences, Associate Professor, Senior Researcher of the Military institute (of national defense) of the Military academy of the General staff of the Armed Forces of the Russian Federation.

For citation: Yampolsky S.M. Conceptual approach to the improvement of military management bodies functioning based on the use of intelligent systems. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 57–64. doi: 10.24411/2409-5419-2018-10288 (In Russian)

ВУС

Военно-учетный стол

Программный комплекс

- Информационное сопряжение с БД военных комиссариатов и проведение сверки в электронном виде
- Совместимость с Комплексом программно-информационных средств мобилизационной подготовки экономики (КПИС МПЭ), построен на той же платформе и расширяет возможности данного комплекса
- Возможность загрузки картотек из других программ, организация работы в сети
- Авторский надзор за эксплуатацией ПК ВУС для наращивания рабочих функций и совершенствования программного комплекса, гарантийное обслуживание

Воинский учет в организациях:

• Ведение электронных Картотек организаций, филиалов и граждан (по Т-2 и Т-2 ГС);

• Документы необходимые для ведения ВУ в организации (приказ, план работы, журнал проверок, расписки о приеме документов ВУ и др.);

• Создание и печать отчетных документов по установленным формам в соответсвии с Инструкцией ГШ ВС РФ по ведению ВУ в организациях;

• Генерация документов по бронированию.

Первичный воинский учет в органах местного самоуправления:

• Ведение Картотеки организаций зарегистрированных на территории ОМСУ;

• Построение и управление картотекой граждан пребывающих в запасе и призывников в ОМСУ;

• Создание отчетных форм документов и других данных в соответствии с Методическими рекомендациями ГШ ВС РФ по ведению первичного ВУ в ОМСУ;

• Распределение организаций ведущих учет ГПЗ по видам экономической деятельности, формам собственности и численности работающих в ней граждан.

Учет и Бронирование в Межведомственных комиссиях:

• Организация картотеки различных органов РФ от правительства до организации включительно с различными формами учета и отчетности, ведение структуры подчиненности;

• Автоматический расчет форм №6,формы №18 расчет и обобщение суммарной формы №6 за все подотчетные объекты;

• Анализ обеспеченности трудовыми ресурсами;

• Ведение перечня должностей и профессий по бронированию граждан;

• Определение сотрудников подлежащих бронированию, бронирование сотрудников в соответствии с ПДП;

• Заполнение, передача, сбор и обобщение форм ГД.

НПЦ ИРС

Научно-производственный центр
Информационных региональных систем

npcirs.ru

doi: 10.24411/2409-5419-2018-10289

DETERMINATION OF THE READINESS FACTOR OF FIBER OPTICAL COMMUNICATION LINES AT TEMPERATURE IMPACTS ON OPTICAL FIBERS

IGOR V. BOGACHKOV[1]

SERGEY S. LUTCHENKO[2]

ABSTRACT

The operational experience of fiber optical communication lines has shown that the service life time of an optical cable depends on both a mechanical strain in optical fibers and their temperature. Segments of overhead cable line can be subjected to essential temperature changes. Cable elements, means of its fastening, line materials have different heat-expansion indexes. Essential mechanical strains take place in the case of significant changes in temperature due to the uneven expansion of the contacting materials within the fiber. To provide a failure-free service of fiber optical communication lines a steady monitoring of optical fibers is needed for timely detection of suspicious segments. Brillouin reflectometers are applied to detect the optical fiber segments with higher strain and temperature changes. The results obtained confirm that the temperature changes in optical fiber impact the readiness index of fiber optical communication lines. Typical Brillouin traces for optical fiber segments with changed temperature are depicted. The estimation technique of the communication line reliability taking into consideration the temperature impacts on fibers is proposed. Reliability of the communication line is estimated by the readiness index. The investigations were carried out using Markov chain theory. The permitted value of the readiness index is calculated after validation of the communication line states, construction of the graphs and system transitions, estimation the true and observed time in given states. The permitted value allows the frequency of maintenance of communication lines to be determined. Process modeling of signal propagation in the optical fiber enables the performance of the communication line reliability taking into account the above equations to be determined. The employment of the Brillouin reflectometer in the control systems increases its reliability and detects the suspicious segments in optical fibers in advance.

Information about authors:

[1]PhD, Docent, Associate professor of Omsk State Technical University, Senior Member IEEE, Omsk, Russia, bogachkov@mail.ru;

[2]PhD, Docent, Associate professor of Omsk State Technical University, Omsk, Russia, lutchenko_s@inbox.ru

KEYWORDS: optical fiber, strain; fiber optic communication line; temperature impact; reliability; mathematical model; readiness factor.

For citation: Lutchenko S.S., Bogachkov I.V. Determination of the readiness factor of fiber optical communication lines at temperature impacts on optical fibers. *H&ES Research*. 2019. Vol. 11. No. 5. Pp. 66–72. doi: 10.24411/2409-5419-2018-10289

The operational experience of fiber optical communication lines (FOCLs) has shown that the service life time of the optical cable depends on both a mechanical strain in optical fibers (OFs) and their temperature [1–3].

Segments of the overhead optical cable can be subjected to essential temperature changes. For example, the optical cable sheath can be heated to a high temperature (about +60 °C) in some segments in summer, and it can be cooled to –40 °C in winter [3–6]. In addition, the temperature of the adjacent segments of optical cable, one of which is under direct sunlight and the other is in the shade, will vary significantly.

This may result in nonreversible changes in the optical fiber in the FOCL because of the higher mechanical strains in the optical fiber, which can reduce the service life time of the optical cable in general [1, 2, 5].

Cable elements (optical fiber, protective members and jackets), means of its fastening, the medium of laying and line materials have different heat-expansion indexes. Essential mechanical strains take place in the case of significant changes in temperature due to the uneven expansion of the contacting materials within the OF [5–8].

To provide a failure-free service of FOCL a steady monitoring of optical fibers is needed for timely detection of suspicious segments [1, 5, 7].

Brillouin optical time domain reflectometers (BOTDRs) are applied to detect the OF segments with higher mechanical strain and temperature changes. The distribution of a Mandelstam — Brillouin backscattering spectrum (MBBS) along the OF is evaluated and assayed in BOTDR [1–3].

In this paper we analyze the Brillouin reflectograms for the segments of optical fibers with changed temperature.

Fig. 1 – Fig. 4 illustrate the Brillouin traces for segments with temperature changes obtained in investigation tests with OFs [1, 5, 7].

In investigation tests, the results of which are given below, the light pipe is composed of single mode optical fibers: G. 652 OF (usual optical fiber), welded with G. 657 fiber, which in turn is welded with G.653 optical fiber (DSF — dispersion-shifted fiber) [5].

Fig. 1 demonstrates the Brillouin reflectogram of the MBBS distribution along the light pipe with heated segments to +90 °C (indicated by solid thick arrows “H”). Solid arrows “1”, “2”, “3” correspond to unheated segments, depending on the OF type: G. 652 — “1” connected to G. 657 OF — “2”, which in turn is welded with G. 653 (DSF) — “3”.

Every cross-section of BOTDR-reflectogram along the distance axis is the reflectogram for a fixed frequency. Every cross-section along the frequency axis is the MBBS profile in this OF section [1, 5]. Both the MBBS peak for the specified line coordinate and the response of MBBS profile in this OF section are depicted in the lower right corner of the reflectogram. For example, the peak of MBBS (f_B — Brillouin frequency shift) is displayed at a frequency of 10.847 GHz in the cross-section of OF at the distance of 949.96 m with a width of MBBS of 193.4 MHz and a level of the received backscattered signal at a maximum of 84.30 dB.

The heated segments occur according to shift of f_B in the direction of a frequency upshift (F2).

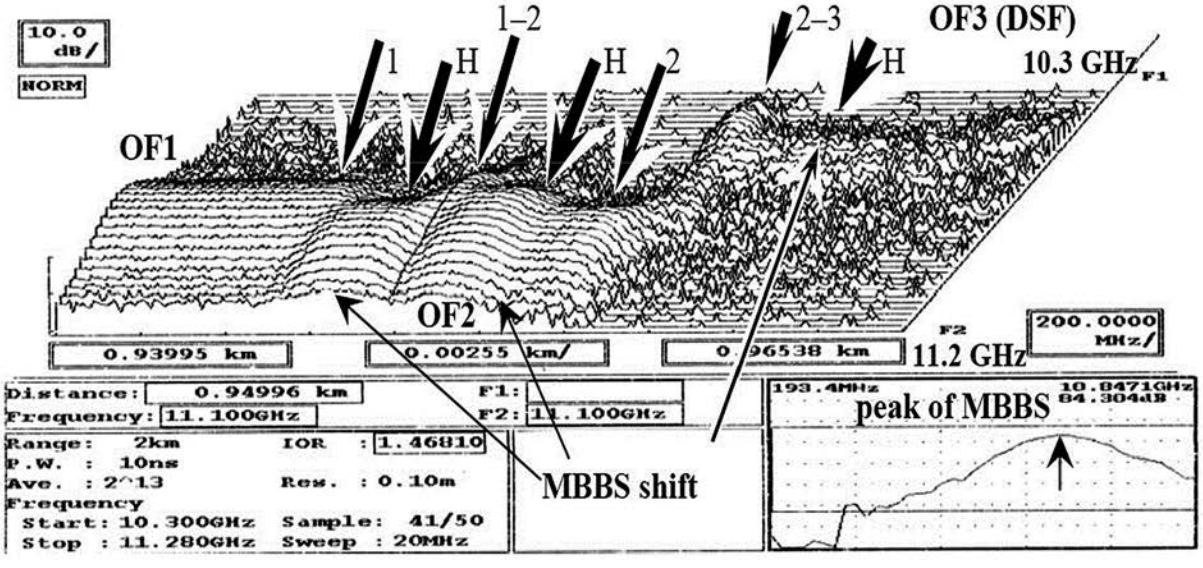


Fig. 1. Trace of the MBBS along a light pipe with heated segments to +90 °

Fig. 2 shows the respective strain pattern in the light pipe (with some heated segments to +90 °C), which is achieved after the MBBS reflectogram processing (Fig. 1).

The tested segments of the light pipe are marked by markers: "1–2" — G. 652, "3–4" — G.657, "5–6" — G.653. Strain values in these segments are distinguished at the bottom of the reflectogram. When evaluating the strain, we use the initial level f_{B0} as a typical value for G. 652 fiber [5, 7].

As a result, the strain in the heated segment for all tested OFs increased by an average of 0.16%.

Fig. 3 shows the strain pattern in the OF with cooled segments of the same light pipe to –10 °C.

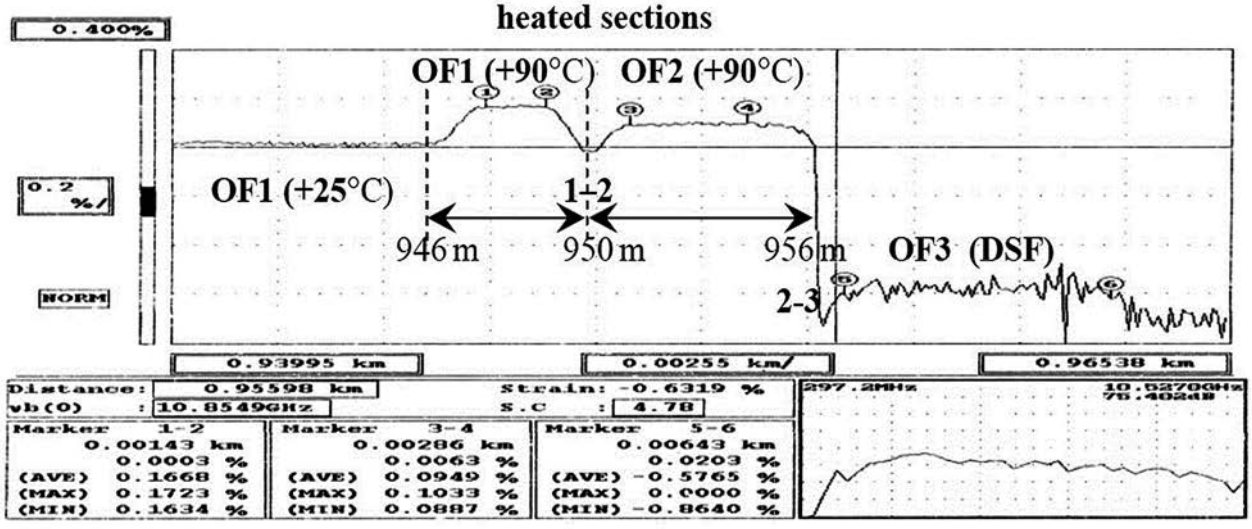


Fig. 2. Strain pattern with heated segments to +90°

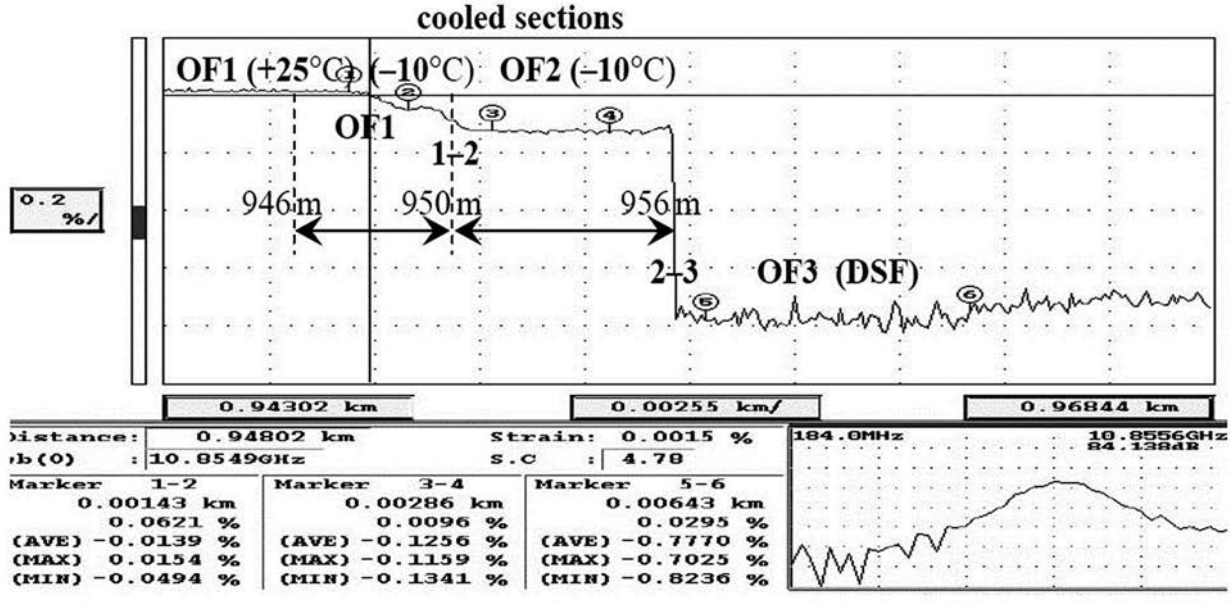


Fig. 3. Strain pattern along the light pipe with cooled segments to –10 °

The frequency downshift f_B is observed in cooled segments.

Evaluation of the strain patterns illustrates a decrease in the OF strain by an average of 0.07% in the cooled segments [5].

As a comparison, the strain pattern in the optical fiber at the room temperature (+25 °C) for the same segments of the light pipe is shown in fig. 4.

Heedless of the fact that the strains in the optical fibers of FOCL are no more than potentially disruptive value (0.2% [1, 5]), the temperature changes in the OFs of the FOCL can alarm the suspicious segments (burst main, cracks in protective structures, unauthorized access, etc.). These phenomena may become a cause of the degradation failure of members of optical cables and fibers, therefore it is necessary to detect them in advance [1–3, 5, 8].

In such a way the impact estimation of this phenomena on the FOCL reliability is of practical interest.

We analyzed the dependence of readiness index of the FOCL on the optical fiber temperature.

The route is seen to be ready for operation if both of its directions are in readiness. There are the following performances of readiness in G.821 recommendation: a readiness index of K_{AF} and an unreadiness index of $K_{U.}$ The readiness index is the ratio of time during which the route is in readiness to the overall period of monitoring. The unreadiness index is the ratio between the time during which the route is in unreadiness and the overall period of monitoring. Markov chain theory and probabilistic mathematical modeling are used to estimate the index [7, 9].

We made the following steps to get a mathematical model.

1. We find out the states in which the FOCL may be located.

2. A graph of states and transitions of the system is constructed.

3. We determine the system transitions from S_i to S_j state.

4. Equations for the readiness index are written.

Fiber optical communication line has following states:

S_0 — operational state;

S_1 — condition under temperature impact on an optical cable;

S_2 — detectable failure state;

S_3 — nondetectable failure state;

S_4 — fictitious failure state;

S_{TO} — maintenance of an operational system;

S_{1TO} — maintenance at temperature impact on the optical cable;

S_{3TO} — maintenance in case of a nondetectable failure.

The graph of conceivable states of the FOCL is illustrated in Fig. 5.

At the time of $t = 0$ the operational system starts working, which is equivalent of the state of S_0. The system operates continuously the time of T (periodicity time or cycle). It is necessary to perform system monitoring and maintenance every time equal to T [10–12].

During operation the system may be subjected to external impacts such as excessive heating or cooling. In this case the system will pass into a state of S_1. At the state of S_1 the overtolerance loads will affect the system and it will fail. In this case, the system will pass into a detectable failure state of S_2. A system failure is a transition to the S_2 state. If during the time T the failure does not occur, the system goes into the state of S_{1TO}. The system is in the state of S_{1TO} for the time $t_п$ required to monitor it. The transition of the system from the state of S_{1TO} to the state of S_2 is possible which corresponds to the system failure.

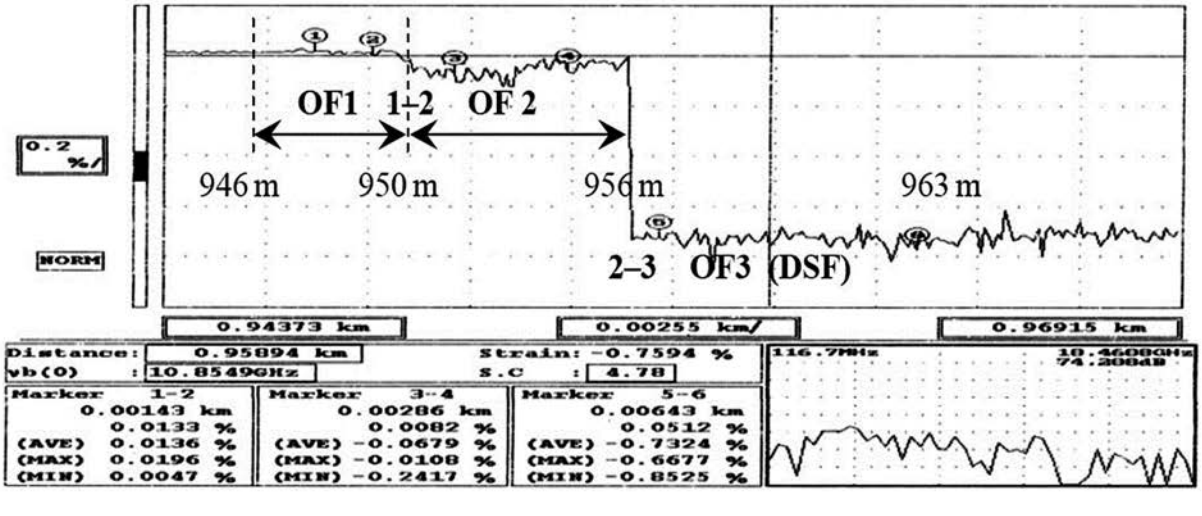


Fig. 4. Pattern of the strain distribution in a light pipe at room temperature

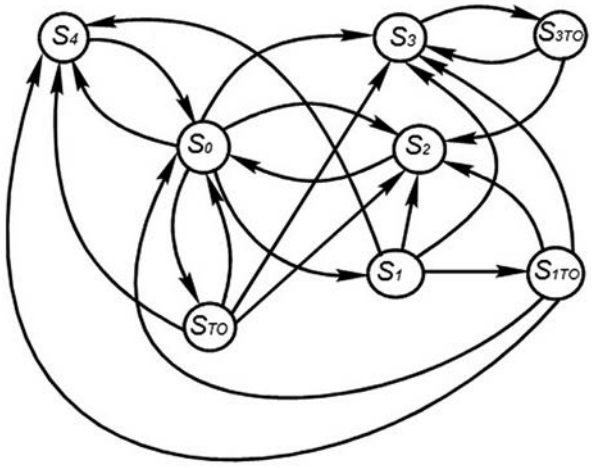


Fig. 5. Graph of states of a FOCL

The transition into the nondetectable failure state is due to the diagnostics error of second type. A possible reason for the system transition from the S_{1TO} to the S_3 is an incorrect choice of performances in the test module (in reflectometer) of the OF monitoring system, leading to a formation of "dead zone" having the non-fixed irregularities. If there is no failure in the S_{1TO} state, the system passes into the operational state of S_0 after that the operating cycle is repeated.

If the system operates a time no more than T in the state of S_0 and then fails, it means that system will pass into a detectable failure state of S_2. If the system operates properly the time T in the state of S_0, it will pass into the maintenance of an operational system of S_{TO}. In this state the system is monitored for a time t_p.

Here we consider a nondetectable failure state of S_3. The system goes into this state only when it is monitored and the system is in it until the next check In this situation, it will obviously pass into the maintenance in case of a nondetectable failure of S_{3TO}. During the test, the nondetectable failure will be detected and then the system will go to a detectable failure state of S_2 and then it will return into the S_0. If the failure is unfound, the system will return into the state of S_3. The return cause of the system to the nondetectable failure state of S_2 is error β_2.

The system has a fictitious failure state of S_4. Fictitious failure occurs due to the diagnostics error of first type of built-in diagnostic equipment. Timely detection of the fictitious failure returns the system to its initial state. Each time when the system returns to the state of S_0 the operating cycle is repeated.

The technique of determination of the readiness index is considered in detail in [7, 12].

The readiness index is found by the following algorithm:

1. The matrix of transition probabilities (P) is written in accordance with the graph of system states (fig. 5).

2. A row matrix of final probabilities (π) is determined [7, 9, 12].

$$\pi = \left|\pi_0(T), \pi_1(T), \pi_2(T), \pi_3(T), \pi_4(T)\right|. \quad (1)$$

3. The final probabilities of the system in each state are determined. In order find it we need to multiply the matrix of transition probabilities by the row matrix of final probabilities and perform the necessary transformations [11, 12].

$$\begin{cases} \pi = \pi \cdot P \ , \\ \sum \pi_i = 1 \end{cases} . \quad (2)$$

4. To determine the readiness index of the FOCL is necessary to estimate the real time of $\omega_i(T)$ and the current time of $\upsilon_i(T)$ for the system in certain states.

The real time is found for the following states: S_0, S_1 and S_4.

$$\omega_i(T) = \sum_j p_{ij} \int_0^{\tau} \tau_{ij} dF_{ij}(\tau_{ij}), \quad (3)$$

where p_{ij} is the transition probability from this state,

τ_{ij} is the time for a system in this state,

$F_{ij}(\tau_{ij})$ is the distribution function for this step of process [1,7, 12].

The current time is determined for the following states: S_0, S_1, S_2, S_3 and S_4.

$$\upsilon_i(T) = \sum_j p_{ij} \int_0^{\tau} \tau_{ij} dF_{ij}(\tau_{ij}). \quad (4)$$

To calculate the readiness index of $K_{AF}(T)$ we use the above functions for the final probabilities $\pi_i(T)$ (1) — (2), for the real $\omega_i(T)$ (3) and the current $\upsilon_i(T)$ (4) time.

An equation for the readiness index of $K_{AF}(T)$ is given by:

$$K_{AF}(T) = \frac{\pi_0(T)\omega_0(T) + \pi_1(T)\omega_1(T) + \pi_4(T)\omega_4(T)}{\pi_0(T)\nu_0(T) + \pi_1(T)\nu_1(T) + \pi_2(T)\nu_2(T) + \pi_3(T)\nu_3(T) + \pi_4(T)\nu_4(T)}. \quad (5)$$

The method for calculation of the reliability performances is difficult and time-taking process. To find the reliability performances we apply the mathematical programs ("MathCAD"), which have the possibility of both numerical and symbolic solution of many tasks, having a mathematical apparatus to calculate the linear algebraic equations [7, 11, 12].

Using the results achieved after calculation, a dependence graph of $K_{AF}(T)$ is constructed, which may be useful for us to determine an allowable time between checks.

Fig. 6 shows the dependency graphs of $K_{AF}(T)$ on temperature of OF obtained using modeling, which enable us to confirm temperature impacts of the OF on the readiness index of the FOCL.

The graphs are presented for three various temperatures of OF: the first value ("1") corresponds to +25 °C (room temperature), the second ("2") — +60 °C, the third ("3") — minus 40 °C.

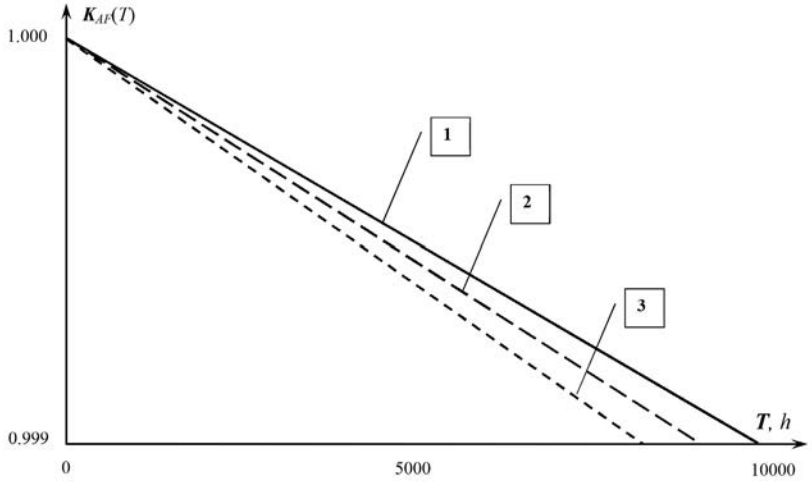


Fig. 6. Dependency graph of $K_{AF}(T)$ on temperature of OF

The conducted tests show that temperature changes in OF impact the reliability performances of FOCL [7, 12].

Process modeling of optical signal propagation in an OF enables the performance of FOCL reliability taking into account the above equations to be determined.

The employment of the BOTDR in the FOCL sensitively increases its reliability and detects the suspicious segments in OFs in advance.

The work was carried out with the financial support of the Ministry of Education and Science of the Russian Federation within the scope of the base part of a State Assignment within the sphere of scientific activity (Project No. 8.9334.2017/8.9).

References

1. Bogachkov I.V., Lutchenko S.S., Kopytov E.Y. Determination of the availability factor of fiber optic communication lines depending on external actions and diagnosis errors. *T-comm.* 2018. Vol. 12. No. 6. Pp. 51–55.

2. Kobyakov A., Sauer M., Chowdhury D. Stimulated Brillouin scattering in optical fibers. *Advances in Optics and Photonics*. 2010. Vol. 2. Issue 1. Pp. 1–59.

3. Bao X., Chen L. Recent Progress in Brillouin Scattering Based Fiber Sensors. *Sensors.* 2011. Vol. 11. Pp. 4152–4187.

4. Lyubchenko A.A., Kopytov E.Y. Determination of preventive maintenance reasonable intervals for moving constraint systems. *Instruments and Systems: Monitoring, Control, and Diagnostics*. 2012. No. 1. Pp. 20–24.

5. Bogachkov I.V. Temperature Dependences of Mandelstam — Brillouin Backscatter Spectrum in Optical Fibers of Various Types. *Proceedings of the conference Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO-2017)*, Kazan, Russia, 3–4 July 2017. New York: Curran Associates, Inc, 2017. Vol. 8. No. 1. Pp. 50–55.

6. Zou W., Long X., Chen J. Brillouin Scattering in Optical Fibers and Its Application to Distributed Sensors. *In book: Advances in Optical Fiber Technology: Fundamental Optical Phenomena and Applications.* Intech, 2015. Chapter 1. Pp. 1–53.

7. Bogachkov I.V., Lutchenko S.S. Reliability assessment of fiber optic communication lines depending on external factors and diagnostic errors. *Journal of Physics: Conference Series. International Conference Information Technologies in Business and Industry*, *Tomsk, 17–20 January 2018.* New York: Curran Associates, Inc, 2018. Vol. 1015. Pt.1. Pp. 26–32.

8. Ruiz-Lombera R., Fuentes A., Rodriguez-Cobo L., Lopez-Higuera J. M., Mirapeix J. Simultaneous temperature and strain discrimination in a conventional BOTDA via artificial neural networks. *Journal of Lightwave Technology*. 2018. Vol. 36. No. 11. Pp. 2114–2120.

9. Lyubchenko A., Castillo P.A., Mora A.M., García-Sánchez P., Arenas M.G. Simulation approach for optimal maintenance intervals estimation of electronic devices *Automation Control Theory Perspectives in Intelligent Systems: Proceedings of the 5th Computer Science On-line Conference 2016 (CSOC2016). Series: Advances in Intelligent Systems and Computing*. Springer, Cham, 2016. Vol. 466. Pp. 153–164.

10. Minardo A., Bernini R., Zeni L. Bend-Induced Brillouin frequency shift variation in a single-mode fiber. *IEEE Photonics Technology Letters.* 2013. Vol. 25. No. 23. Pp. 2362–2364.

11. Maistrenko V.A., Bogachkov I.V. Kopytov E.Y., Lyubchenko A.A., Lutchenko S.S. Castillo P.A. An approach for estimation of integrated reliability indices and maintenance intervals of fiber-optic communication lines. *Proceedings of the conference Actual Problems of Electronic Instrument Engineering*, Novosibirsk, 03–06 October 2016. Novosibirsk, 2016. Vol. 1. Pp. 64–68.

12. Lutchenko S.S., Kopytov E.Y., Bogachkov I.V. Assessment Of Fiber Optic Communication Lines Reliability With Account Of External Factors Influence. *Proceedings of the conference* IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics), Omsk, Russia, 13–15 November 2018. Omsk, 2017. Pp. 1–5.

ОПРЕДЕЛЕНИЕ КОЭФФИЦИЕНТА ГОТОВНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ ПРИ ТЕМПЕРАТУРНЫХ ВОЗДЕЙСТВИЯХ НА ОПТИЧЕСКИЕ ВОЛОКНА

ЛУТЧЕНКО Сергей Святославович,
Омск, Россия, lutchenko_s@inbox.ru

БОГАЧКОВ Игорь Викторович,
Омск, Россия, bogachkov@mail.ru

KEYWORDS: оптическое волокно; натяжение; волоконно-оптическая линия связи; температурное воздействие; надёжность; математическая модель; коэффициент готовности.

АННОТАЦИЯ

Практика эксплуатации волоконно-оптических линий связи (ВОЛС) показала, что срок службы оптического кабеля зависит от механических натяжений его оптических волокон (ОВ), а также от их температуры. Участки кабелей, проложенных с использованием подвесной технологии, могут испытывать существенные перепады температуры. Например, летом оболочка кабеля может на некоторых участках нагреваться до высокой температуры, а зимой может сильно охлаждаться. Это может привести к необратимым изменениям в ОВ ВОЛС, связанным с появлением повышенных механических напряжений в ОВ, что может значительно сократить срок службы кабеля в целом. Элементы кабеля, средства его крепежа, среда прокладки и материалы линии имеют различные коэффициенты теплового расширения. В случае существенных изменений температуры из-за неравномерного расширения соприкасающихся материалов внутри ОВ также могут возникать существенные механические натяжения. ля обеспечения бесперебойной работы ВОЛС необходим постоянный мониторинг ОВ для своевременного выявления проблемных участков. Для обнаружения напряжённых участков ОВ или имеющих изменённую температуру, применяются бриллюэновские оптические импульсные рефлектометры (БОИР). На основании проведённых оценок можно сделать вывод, что изменение температуры ОВ оказывает влияние на показатели готовности ВОЛС. Приведены характерные БОИР-графики участков ОВ с изменённой температурой. Рассмотрена методика оценки надёжности ВОЛС с учётом влияния температуры на её ОВ. Надёжность ВОЛС оценивается по коэффициенту готовности. Исследования выполнены с применением теории цепей Маркова и вероятностного математического моделирования. Допустимое значение коэффициента готовности определяется после обоснования состояний ВОЛС, составления графов и переходов системы, вычисления истинного и наблюдаемого времени нахождения системы в заданных состояниях, и позволяет определить предельную периодичность обслуживания ВОЛС. Моделирование процессов распространения оптического сигнала в ОВ с учетом приведенных формул позволяет определить характеристики надежности ВОЛС. Включение БОИР в систему мониторинга ВОЛС существенно повышает её надёжность, так как позволяет заблаговременно обнаруживать проблемные участки в ОВ.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части госзадания в сфере научной деятельности (проект № 8.9334.2017/8.9).

СВЕДЕНИЯ ОБ АВТОРАХ:

Лутченко С.С., к.т.н., доцент; доцент Омского государственного технического университета;

Богачков И.В., к.т.н., доцент; доцент Омского государственного технического университета, Член IEEE.

Для цитирования: *Лутченко С.С., Богачков И.В.* Определение коэффициента готовности волоконно-оптических линий связи при температурных воздействиях на оптические волокна // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 66–72. doi: 10.24411/2409-5419-2018-10289