H&ES RESEARCH

WWW.H-ES.RU

ISSN 2409-5419 (Print)
ISSN 2412-1363 (Online)

Научно-технический журнал
2018. Т. 10. № 6

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

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.

Scientific and Technical Journal
2018. Vol. 10. No. 6

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

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.

HES_Research club55425245 HES-Research

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

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

РАДИОТЕХНИКА И СВЯЗЬ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ПУБЛИКАЦИИ НА АНГЛИЙСКОМ ЯЗЫКЕ ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

CONTENTS

Founder:
"Media Publisher", LLC

Publisher:
SVETLANA DYMKOVA

Editor in chief:
KONSTANTIN LEGKOV

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: 10.24411/2409-5419-2018-10183

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННО-ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ МАГИСТРАЛЬНО-МОДУЛЬНЫХ БОРТОВЫХ НАВИГАЦИОННО-ПОСАДОЧНЫХ КОМПЛЕКСОВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

БЕЗЗУБОВ
Владимир Федорович[1]

КРИВОРУЧКО
Юрий Тимофеевич[2]

МУЗЕЛИН
Юрий Николаевич[3]

АННОТАЦИЯ

В работе рассмотрены методы обеспечения информационно-функциональной безопасности магистраль-модульных бортовых навигационно-посадочных комплексов специального назначения на основе межмашинного прямого доступа к памяти, а также аппаратных средств реконфигурации структуры комплекса в случае сбоя либо отказа. Проведен анализ организации информационного обмена между вычислительными модулями в комплексах реального времени на основе технологии RDMA Consortium, высокоскоростного интерфейса SRIO и межмашинного прямого доступа к памяти межмашинного прямого доступа к памяти. Показано, что в соответствии с принципом импортозамещения, для организации высокоскоростного информационного обмена в бортовых навигационно-посадочных комплексах наиболее эффективно применение отечественного способа организации обмена данными – межмашинного прямого доступа к памяти, реализующего конвейерную передачу данных, по сравнению с технологии RDMA Consortium, а также интерфейсом SRIO, разработанным компаниями Texas Instruments, Freescale, Semiconductor и др. Произведен сравнительный анализ временных характеристик восстановления вычислительного процесса, после возникновения отказа, в системах реального времени, построенных на основе последовательного интерфейса RapidIO – SRIO и на основе интерфейса межмашинного прямого доступа к памяти. Показано, что в соответствии с принципом импортозамещения, для сокращения времени восстановления вычислительного процесса после возникновения отказа, в системах реального времени, наиболее эффективно применение отечественного способа организации обмена данными – межмашинного прямого доступа к памяти, реализующего конвейерную передачу данных, по сравнению с интерфейсом SRIO, применяемым зарубежными компаниями. Приведены результаты сравнительного анализа применения аппаратных и программных средств организации восстановления работоспособности бортовых навигационно-посадочных комплексов после возникновения отказа методом реконфигурации структуры. Показано, что использование аппаратных средств контроля и управления реконфигурацией структуры в сочетание с межмашинным прямым доступом к памяти позволяет повысить эффективность обеспечения информационно-функциональной безопасности бортовых навигационно-посадочных комплексов специального (военного) назначения..

КЛЮЧЕВЫЕ СЛОВА: надёжность; безотказность; доступность; избыточность; готовность; ремонтопригодность; отказоустойчивость; безопасность; бортовой навигационно-посадочный комплекс.

Сведения об авторах:

[1]к.т.н., с.н.с. акционерного общества «Ордена Трудового Красного Знамени Всероссийский научно-исследовательский институт радиоаппаратуры», г. Санкт-Петербург, Россия, bezzubov_vf@mail.ru

[2]к.т.н., начальник сектора акционерного общества «Ордена Трудового Красного Знамени Всероссийский научно-исследовательский институт радиоаппаратуры», г. Санк-Петербург, Россия, krivoruchko.yuri@mail.ru

[3]к.т.н., начальник отдела акционерного общества «Ордена Трудового Красного Знамени Всероссийский научно-исследовательский институт радиоаппаратуры», г. Санк-Петербург, Россия, yuri.muzelin@gmail.com

Для цитирования: *Беззубов В.Ф, Криворучко Ю.Т., Музелин Ю.Н.* Обеспечение информационно-функциональной безопасности магистрально-модульных бортовых навигационно-посадочных комплексов специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 4–18. doi: 10.24411/2409-5419-2018-10183

При проектировании и построении бортовых навигационно-посадочных комплексов (БНПК) специального назначения создание средств, обеспечивающих устойчивое функционирование вычислительных модулей, сокращение риска потери функциональности системы и последствий потери информации, после случайных или злонамеренных дестабилизирующих воздействий, является актуальной задачей.

Обеспечение информационно-функциональной безопасности [1], прежде всего, связано с минимизацией риска потери данных при отказах БНПК, вызванных внешними или внутренними причинами, в том числе в результате злонамеренных воздействий.

Для снижения риска потери данных и критических результатов вычислений в системах ответственного (критического) назначения, как правило, производится резервирование основных ресурсов обработки и хранения данных, что приводит к реализации вычислительных узлов в виде резервированных, в том числе дублированных, вычислительных комплексов (ДВК).

Эффективность средств защиты от внешних и внутренних воздействий, вызывающих нарушение целостности информации и отказы систем управления, во многом определяется организацией средств комплексирования, которые должны обеспечить высокоскоростной доступ к памяти, хранящей важные для вычислительного процесса данные и результаты вычислений. Высокоскоростной доступ к ресурсам вычислительных комплексов, позволяет ускорить контроль и обнаружение опасных состояний, минимизировать их вероятности и увеличить эффективность процесса снижения риска компенсацией ошибочного функционирования вычислительного процесса, потери доступности и целостности данных.

1. В работах [2–3] рассмотрены вопросы организации межмашинного обмена и получены следующие временные характеристики для ДВК при различной организации взаимосвязи вычислительных модулей (ВМ):

– обмен через радиальные соединения:

$$T_{\text{рс.}} = T_{\text{ор}} + 4tN;$$

– обмен через общую память (ООЗУ):

$$T_{\text{оп}} = 4t\,N;$$

– обмен через адаптер «канал — канал»:

$$T_{\text{к-к}} = T_{\text{ор}} + 2tN, \text{ или для Q — шины: } 9t + 2tN = 2t(N+4{,}5),$$

где t —среднее время одного процессорного цикла шины (ввод/вывод, чтение/запись), N — количество слов информационного массива, $T_{\text{ор}}$ — время организации режима обмена.

Из рассмотренных вариантов организации обмена наименьшее время передачи информации может быть получено при объединении, через адаптер «канал — канал», внутренних магистралей (ВнМ) вычислительных модулей (ВМ), участвующих в обмене.

Рассмотренное в работе [4] техническое решение позволяет сократить время информационного обмена между отдельными, входящими в комплекс вычислительными модулями, за счет организации межмашинного (двойного) прямого доступа к памяти (мПДП), обеспечивающего доступ к памяти вычислительного устройства с отказавшим процессором, в результате чего появляются дополнительные возможности обеспечения доступности, целостности информации, отказоустойчивости микропроцессорных магистрально-модульных БНПК [5–7].

При использовании двойного ПДП время, затрачиваемое на передачу массива из N слов, составляет: $T_{\text{ууо}} = T_{\text{ор}} + t(N+1)$; при этом для Q — шины $T_{\text{ууо}} = t(N+16)$; где t — цикл шины [3]. Применение двойного ПДП, по сравнению с обменом через общую память и адаптером «канал — канал», не поддерживающим двойной ПДП, позволяет сократить время обмена. Действительно, при обмене через общую память требуется время: $T_{\text{оп}} = 4tN$, а при обмене через адаптер «канал — канал»: $T_{\text{к-к}} = T_{\text{ор}} + 2tN$. При этом, например, для магистрали типа «Q — шина» $T_{\text{ор}} = 9t$ и соответственно $T_{\text{к-к}} = 2t(N+4{,}5)$ [3]. Эффективность двойного ПДП относительно обмена через общую память и адаптер «канал — канал» определим, соответственно, как $k_1 = T_{\text{к-к}} / T_{\text{ууо}}$; $k_2 = T_{\text{оп}} / T_{\text{ууо}}$ (рис. 1).

Применение двойного ПДП целесообразно, когда время организации режима обмена меньше времени передачи массива информации программным способом: $T_{\text{ор}} \le 4tN$, что соответствует $N \ge 4$.

В работе [8] определена зависимость времени восстановления вычислительного процесса ДВК от способа организации обмена между полукомплексами (ВМ). В работе [8] показано:

$$t_{\text{ввп}} \ge t_{\text{икт}} + t_{\text{вк}} + t_{\text{зкт}}; \text{ отсюда: } t_{\text{икт}} = t_{\text{ввп}} - t_{\text{вк}} - t_{\text{зкт}},$$

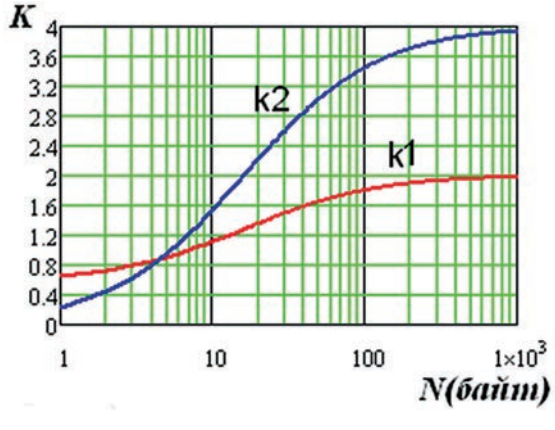


Рис. 1. Относительная эффективность двойного ПДП

где $t_{ввп}$ — время восстановления вычислительного процесса после отказа; $t_{икт}$ — величина интервала времени передачи данных контрольных точек (КТ); $t_{вк}$ — время взаимоконтроля ВМ; $t_{зкт}$ — время загрузки данных КТ.

Потеря производительности ДВК при реализации передачи информации о КТ составит:

$$T^* = t_{пкт} / t_{ввп} - t_{вк} - t_{зкт},$$

где $t_{пкт}$ — время передачи данных КТ, или:

– для структуры с общей памятью:

$$T_{оп} = \frac{8Q_1N_{км}(1/F_ω)}{t_{ввп} - 16Q_1N_1(1/F_ω)};$$

– для структуры с адаптером «канал — канал»:

$$T^*_{ммк} = \frac{4Q_1(N_{км}+4)(1/F_ω)}{t_{ввп} - 8Q_1(N_1+4)(1/F_ω) - 8N_{км}/F_ω};$$

– для структуры с адаптером (УУО):

$$T^*_{ууо} = \frac{4Q_1(N_{км}+4)(1/F_ω)}{t_{ввп} - 8Q_1(N_1+4)(1/F_ω) - 8N_{км}/F_ω};$$

здесь Q — коэффициент, характеризующий способ организации ввода/вывода.

Для расчёта принято: $F_ω$ = 200 МГц — частота шины, Q_1 = 1 (для ввода/вывода без ПДП, когда ЦП непосредственно участвует в каждой операции пересылки), Q_2 = 0,7 (для ввода/вывода с ПДП, когда ЦП участвует лишь в инициализации КПДП и формировании сигнала «подтверждение ПДП»), N_1 = 1, $N_{км}$ = 1000000:

Результаты расчетов показаны на рис. 2.

При потере производительности системы T = 5% время восстановления вычислительного процесса составляет:

$t_{Воп}$ = 1,734 с; $t_{Вммк}$ = 0,893 с; $t_{Вууо}$ = 0,27 с;

Минимальное время восстановления вычислительного процесса ДВК достигается при организации обмена с использованием межмашинного (двойного) ПДП.

При передаче больших массивов данных с использованием режима двойного ПДП возможно их разбиение на кадры с организацией режима работы для каждого кадра.

Разбиение передаваемого массива данных на кадры приводит, с одной стороны, к снижению вероятностей повторных передач из-за сбоев и соответственно к сокращению временных затрат на повторные передачи, а с другой стороны — к возрастанию издержек времени на организацию каналов прямого доступа. Соответственно возникает задача оптимизации числа кадров, формируемых при передаче массива данных в режиме двойного ПДП.

Среднее время межмашинного обмена (T) с установлением канала двойного ПДП при разбиении передаваемого массива данных, состоящего из N слов, на k кадров вычисляется как [9]:

$$T = \left((1+N/k)t+d\right)k\sum_{i=1}^{\infty} ib(1-b)^{i-1}$$

где $b = e^{-((1+N/k)t+d)(\lambda 2+\lambda 3)}$

Зависимость времени T от числа кадров k, формируемых при передаче массива данных длиной N слов, представлена на рис. 3.

Полученные результаты показывают наличие в режиме межмашинного (двойного) ПДП оптимального числа кадров, формируемых при передаче массива данных,

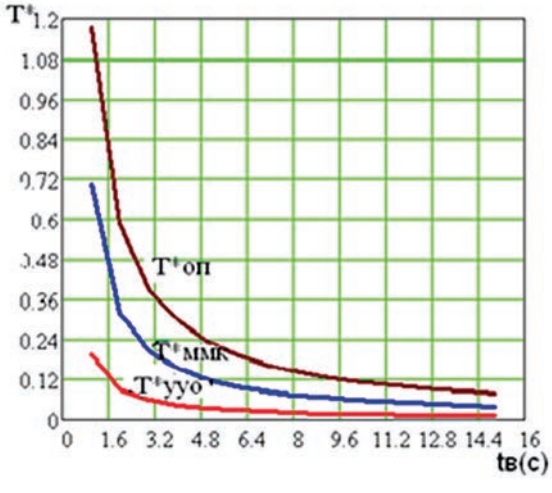


Рис. 2. Время восстановления вычислительного процесса

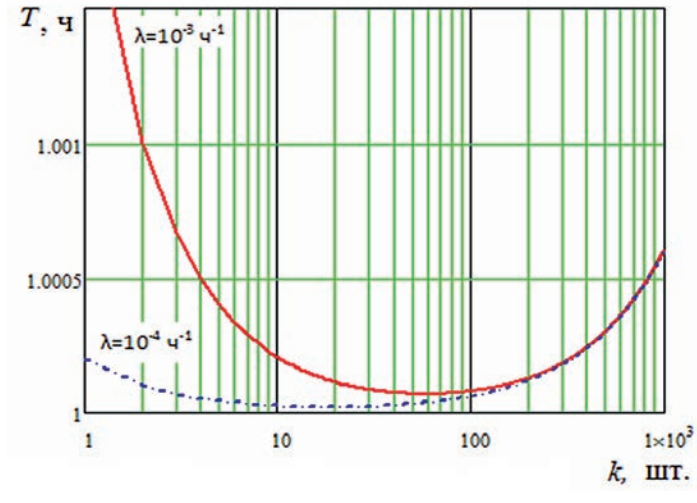


Рис. 3. Оптимизация длины кадров информационного массива

при котором, в условиях сбоев, время межмашинного обмена минимально.

Рассмотренное техническое решение, при создании управляющих вычислительных комплексов (систем), позволяет:

– повысить скорость параллельных вычислений в двухмашинных (многомашинных) вычислительных комплексах за счет сокращения времени информационного обмена, между вычислительными модулями комплекса;

– сократить время обмена информацией, что уменьшает вероятность возникновения сбоя при обмене и, соответственно, повышает сохранность информациипри обмене;

– сократить время обнаружения опасных состояний и выхода из них, т.е. минимизировать вероятность возникновения опасных состояний;

– получить дополнительные временные ресурсы, которые могут быть использованы для повышения живучести ВК посредством реализации различных вариантов избыточности, что особенно важно при создании ВК, работающих в режиме реального времени;

– обеспечить доступ к памяти вычислительного устройства с отказавшим процессором, в результате чего появляются дополнительные возможности обеспечения информационно — функциональной безопасности, отказоустойчивости и живучести вычислительных комплексов и систем управления, что позволяет повысить устойчивость функционирования резервированных комплексов путем создания работоспособных конфигураций, с использованием сохраненных после деструктивных воздействий (отказов) ресурсов и результатов вычислений.

В настоящее время ни одна из отечественных систем подобными свойствами не обладает.

Таким образом, применение межмашинного (двойного) ПДП, для организации информационного обмена, позволяет повысить информационную безопасность автоматизированных систем управления и обеспечить их устойчивое функционирование при случайных или злонамеренных дестабилизирующих воздействиях.

2. В резервированных (дублированных) вычислительных комплексах (ДВК), при выходе из строя основного вычислителя, исправные вычислительные устройства берут на себя функции вышедшего из строя, тем самым обеспечивая надежное функционирование вычислительного комплекса.

Немаловажное значение имеет время восстановления работоспособности вычислительного комплекса после отказа, которое зависит от организации контроля работоспособности вычислительных модулей (ВМ) комплекса, а также от реализации механизма реконфигурации структуры в случае возникновения отказа.

Для контроля работы вычислительных устройств и управления реконфигурацией в многомашинных вычислительных комплексах (ММВК), объединяющих ВМ с АКВИ (автоматом контроля и восстановления информации), требуется разработка и совершенствование блоков контроля и управления резервированием (БКУР), представляющих собой процессорные устройства с повышенными требованиями к надежности.

В структурах с АМКВИ (автоматом межмашинного контроля и восстановления информации) для обеспечения синхронизации процессов в ВМ и организации информационного обмена между ВМ требуется использование высокоскоростных сетевых интерфейсов необходимых для обеспечения дополнительного ресурса времени, позволяющего реализовать программные методы внутреннего тестирования и межмашинного контроля. Сокращение времени информационного обмена может быть достигнуто при использовании межмашинного прямого доступа к памяти (мПДП).

В работе [9] рассматривается применение в управляющих вычислительных комплексах (системах) устройства управления реконфигурацией (УР), которое позволяет частично возложить функции контроля работоспособности вычислительных модулей и реконфигурации структуры вычислительного комплекса (системы) на аппаратные средства.

При этом в каждом ВМ комплекса (системы), специальная программа, на основании анализа тестов формирует своё «слово — состояния» ВМ и передает его в УР. На основании полученной информации, УР вырабатывает, на аппаратной логике, признак «ведущий» для одного из ВМ комплекса (системы).

Время контроля работоспособности вычислительных модулей определяется передачей вычислительными модулями коротких сообщений о результатах тестового самоконтроля в УР. При этом потеря производительности комплекса определяется отношением времени пересылки сообщений между ВМ и УР, к интервалу времени между посылками — $t_{\text{ио}}$.

Показано, что потеря производительности вычислительного комплекса (ДВК), обусловленная реализацией обмена между ВМ и УР, составит:

– при поочередном обмене между ВМ комплекса и УР:

$$T^{*}_{\text{ур}} = 16 Q_1 N_1 (1/F_{\text{ш}})/t_{\text{ио}}$$

– при синхронном обмене между ВМ комплекса и УР:

$$T^{*}_{\text{ур1}} = 8 Q_1 N_1 (1/F_{\text{ш}})/t_{\text{ио}}$$

здесь Q — коэффициент, характеризующий способ организации ввода/вывода,$F_{\text{ш}}$ — частота шины, N_1 — величина передаваемого массива информации.

Видим, что при синхронном обмене, т.е. при одновременном обращении ВМ комплекса к УР, время, затрачиваемое на обмен, сокращается вдвое.

Сравним данный способ контроля работоспособности ВМ комплекса с контролем работоспособности, основанным на обмене сообщениями между ВМ.

При обмене сообщениями между ВМ комплекса потеря производительности определяется способом организации обмена между ВМ [3].

С учётом временных затрат на пересылку сообщений в обе стороны потеря производительности комплекса, обусловленная взаимоконтролем, выражается как:

– для структуры с общей памятью;

$$T^*_{\text{оп}} = 32Q_1N_1(1/F_{\text{ш}})/t_{\text{ио}}$$

– для структуры с адаптером канал — канал;

$$T^*_{\text{ммк}} = 16Q_1(N_1+4)(1/F_{\text{ш}})/t_{\text{ио}}$$

– для структуры с адаптером, реализующим межмашинный (двойной) ПДП;

$$T^*_{\text{увв}} = 8Q_2^2\left(N_1+16\right)(1/\ F_{\text{ш}})/t_{\text{ио}}$$

Для расчёта принято: Q=1 (для ввода/вывода без ПДП, когда ЦП непосредственно участвует в каждой операции пересылки), Q = 0,7 (для ввода/вывода с ПДП, когда ЦП участвует лишь в инициализации контроллера прямого доступа к памяти (КПДП) и формировании сигнала «подтверждение ПДП»), N_1=1, $F_{\text{ш}}$ = 200 МГц,

Результаты расчета представлены на рис. 4.

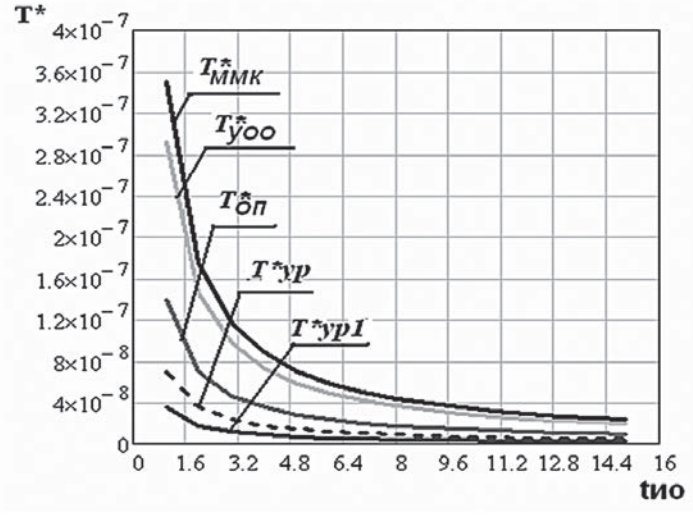


Рис. 4. Зависимость потери производительности ДВК от интервала времени контроля работоспособности ВМ

Таким образом, применение УР позволяет сократить время контроля исправного функционирования вычислительных модулей ДВК.

В работе рассматривается влияние применения УР на время восстановления вычислительного процесса после отказа одного из ВМ.

$$t_{\text{в}} = t_{\text{икт}} + t_{\text{контр}} + t_{\text{рек}},$$

где $t_{\text{контр}}$ — время, затрачиваемое на обмен между ВМ и УР, $t_{\text{икт}}$ — интервал времени передачи данных контрольной точки (КТ), $t_{\text{рек}}$ — время реконфигурации структуры ВМ.

При нарушении работоспособности основного ВМ, время, затрачиваемое на реконфигурацию системы, определяется временем реализации процедуры переключения на резервный ВМ (рис. 5).

В работе [9] показано, что в соответствии с приведенным алгоритмом:

$$t_{\text{рек}} = \tau + 14t,$$

где $t = 4(1/F_{\text{ш}})$; $\tau = 4n/F_{\text{ш}}$, n — количество процессорных циклов необходимых для завершения выполнения процессором команды в момент поступления сигнала требование прерывания (ТПР).

Потеря производительности, обусловленная временем восстановления ДВК, составит:

– при последовательном обмене между ВМ и УР:

$$T^*_{\text{ур}} = \frac{4Q_2{}^2(N_{\text{кт}}+16)(1/F_{\text{ш}})}{t_{\text{ввп}} - 8Q_1N_1(1/F_{\text{ш}}) - (4n/F_{\text{ш}}) - 56(1/F_{\text{ш}})}$$

– при синхронном обмене между ВМ и УР:

$$T^*_{\text{ур1}} = \frac{2Q_2{}^2(N_{\text{кт}}+16)(1/F_{\text{ш}})}{t_{\text{ввп}} - 4Q_1N_1(1/F_{\text{ш}}) - (4n/F_{\text{ш}}) - 56(1/F_{\text{ш}})}$$

Для ДВК без использования УР и организацией программного взаимоконтроля работоспособности ВМ комплекса [8] потеря производительности ДВК составит:

– для структуры с общей памятью:

$$T^*_{\text{оп}} = \frac{16Q_1N_{\text{кт}}(1/F_{\text{ш}})}{t_{\text{ввп}} - 16Q_1N_1(1/F_{\text{ш}})};$$

– для структуры с адаптером «канал — канал»:

$$T^*_{\text{ммк}} = \frac{8Q_1(N_{\text{кт}}+4)(1/F_{\text{ш}})}{t_{\text{ввп}} - 8Q_1(N_1+4)(1/F_{\text{ш}}) - 8N_{\text{кт}}/F_{\text{ш}}};$$

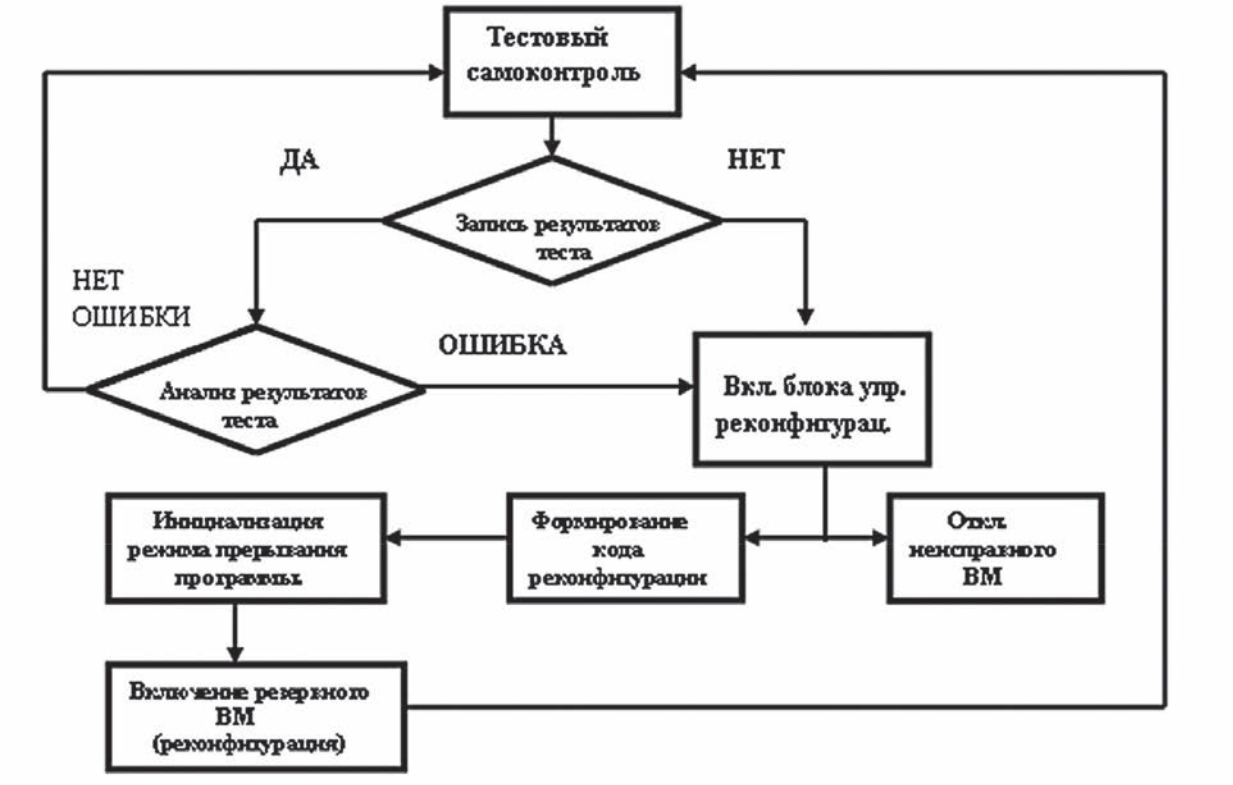


Рис. 5. Алгоритм работы УР

– для структуры с адаптером реализующим межмашинный (двойной) ПДП:

$$T^{*}_{\text{ууо}} = \frac{4Q_2{}^2(N_{\text{кт}}+16)(1/F_{\text{ш}})}{t_{\text{ввп}}4Q^2(N_1+16)(1/F_{\text{ш}})-8N_{\text{кт}}/F_{\text{ш}}};$$

Для расчёта принято: Q = 1, Q = 0,7, N_1 = 1, $N_{\text{кт}}$ = 1000000, $F_{\text{ш}}$ = 200 МГц, n = 10.

При приемлемой потере производительности 5% определено время восстановления вычислительного процесса:

– при организации поочередного обмена между ВМ и УР:

$$t_{\text{Вур}} = [4Q_2^2(N_{\text{кт}}+16)(1/F_{\text{ш}})/T]+8Q_1N_1(1/F_{\text{ш}})+$$
$$+(4n/F_{\text{ш}})+56(1/F_{\text{ш}}) = 0,225 \text{ с}.$$

– при синхронном обмене между ВМ и УР:

$$t_{\text{Вур1}} = [4Q_2^2(N_{\text{кт}}+16)(1/F_{\text{ш}})/T]+4Q_1N_1(1/F_{\text{ш}})+$$
$$+(4n/F_{\text{ш}})+56(1/F_{\text{ш}}) = 0,225 \text{ с}.$$

Для ДВК без использования УР, как показано в работе [13]:

$$t_{\text{Воп}} = 1,734 \text{ с}; t_{\text{Вммк}} = 0,893 \text{ с}; t_{\text{Вууо}} = 0,27 \text{ с};$$

Использование УР для контроля работоспособности ВМ и реконфигурации структуры комплекса в случае нарушения работоспособности ВМ, сокращает время восстановления вычислительного процесса.

Использование дополнительного устройства управления реконфигурацией в сочетании с программным тестовым самоконтролем ВМ, а также организация обмена между ВМ комплекса на основе межмашинного (двойного) прямого доступ к памяти, сокращает время на контроль работоспособности ВМ, время на обмен информацией между ВМ, а также дает возможность работы исправного ВМ с памятью отказавшего ВМ и соответственно повышает сохранность информации и устойчивость работы вычислительного комплекса.

Применение устройства для реконфигурации резервированной системы, при построении многомашинных управляющих комплексов (систем), позволяет создавать управляющие вычислительные комплексы (системы) с программно — перестраиваемой структурой [10].

Вычислительный комплекс (система), с программно — перестраиваемой структурой, представляет собой объединение узловых вычислителей (УВ), функциональное взаимодействие между которыми осуществляется через программно — перестраиваемую коммуникационную среду (КС), состоящую из модуля контроля и управления реконфигурацией (МКиУ) и блока реконфигурации (БР).

На рис. 6. показана упрощенная структурная схема многомашинного вычислительного комплекса (системы) с программируемой структурой.

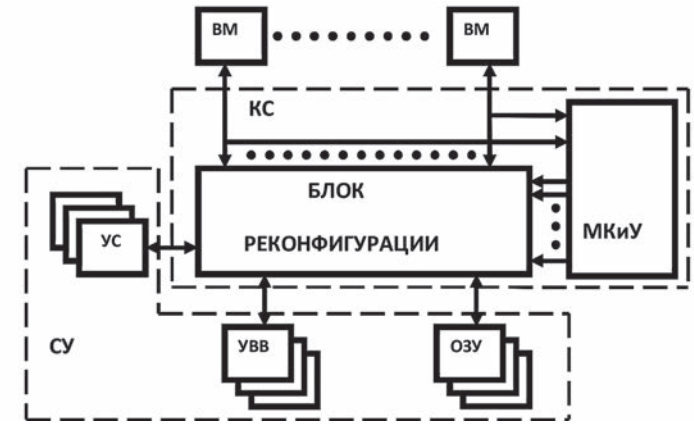


Рис. 6. ММВК с программируемой структурой

Каждый из узловых вычислителей комплекса способен выполнять любые процессы, иметь доступ ко всем каналам ввода-вывода и, в случае необходимости, как полностью, так и частично дублировать работу любого другого узлового вычислителя и составляющих устройств, реализуя, тем самым, метод гибкого резервирования замещением. Полный доступ к внутренним ресурсам узловых вычислителей позволяет сократить время восстановления системы после отказа, а значит повысить коэффициент готовности системы. Полное резервирование аппаратных средств обеспечивает отсутствие «изолированных мест повреждения» в системе [11].

3. Необходимость использования ПДП для организации информационного обмена между отдельными компьютерами вычислительной системы продиктована увеличением скорости потока данных в современных каналах связи, что привело к возникновению идеи RDMA — Remote Direct Memory Access (дистанционный ПДП).

Разработка технологии использования ПДП для организации информационного обмена между отдельными компьютерами велась под управлением RDMA Consortium, куда входят многие гранды индустрии, такие как IBM, Cisco, NetApp, EMC, HP, Intel, Microsoft, общим числом около 50. Работы велись с 1998 года, а в 2003 году RDMA Consortium объявил о завершении всех запланированных спецификаций.

Использование сетевых адаптеров RDMA основано на реализации функции SMB Multichannel, которая является частью сетевого протокола SMB3.0. SMB Multichannel отвечает за обнаружение поддержки RDMA сетевого адаптера.

В работе [12] определено время передачи информации при использовании RDMA — канала:

$$T_{\text{RDMA}} = T_{\text{ор. канала}} + T_{\text{передачи}},$$

где $T_{\text{передачи}} = 4tN$ — при условии передачи данных без учета времени прохождения сигнала через канал объединяющий сетевые адаптеры, где t — цикл шины (ввод/вывод), N — количество слов информационного массива, $T_{\text{ор. канала}}$ — определяется временными издержками на реализацию функции SMB Multichannel (T_{SMBm}), которая является частью протокола SMB3.0. и временем организации режима ПДП ($T_{\text{ор/пдп1;2}}$), т. е.

$$T_{\text{ор. канала}} = T_{\text{SMBm}} + T_{\text{ор/пдп1;2}}.$$

При передаче «отмеченных» сообщений в локальном узле клиентский протокол посредством протокола RDDP регистрирует буфер. После регистрации буфера в локальном узле, он становится доступным удаленному узлу. Локальный узел должен послать удаленному узлу параметры буфера и специальный ключ, разрешающий доступ к памяти локального узла. Все эти процедуры увеличивают время организации режима работы RDMA.

Очевидно, что использование дистанционного ПДП (RDMA) требует времени для программной обработки сетевых протоколов при организации режима работы и канала RDMA.

При построении локальных (малых) систем управления применение технологии RDMA Consortium базируется на использовании высокоскоростной коммутируемой последовательной шины Infiniband, применяющейся как для внутренних (внутрисистемных), так и для межсистемных соединений.

Таким образом, использование технологии RDMA Consortium для построения локальных (малых) систем управления требует создания сетевых структур и соответственно дополнительных временных издержек на реализацию TCP/IP- протоколов для организации каналов и режима работы RDMA. Кроме того, применение функции SMB Multichannel протокола SMB3.0 требует использования Windows Server 2012 или Windows 8, что ограничивает номенклатуру применяемого ПО.

Выбор архитектуры системы управления реального времени, адекватной решаемым задачам, является актуальной проблемой. Ошибочные решения, принятые на этапе выбора типов межмашинных (межпроцессорных) интерфейсов, могут стать причиной снижения качественных характеристик системы и необоснованных затрат на ее реализацию.

Сегодня, широкую популярность, в том числе и в ОПК нашей страны, приобрел интерфейс «быстрого ввода-вывода» — RapidIO (SRIO),— одним из авторов его создания и внедрения была компания Texas Instruments. Это совре-

менный интерфейс мультипроцессорных систем с высокой скоростью передачи данных. Он используется для коммуникаций, как между чипами в пределах одной платы, так и между платами в пределах устройства. Вычислительные модули, в данном случае, объединяются высокоскоростными последовательными каналами по принципу «точка — точка», или с использованием коммутаторов.

В работе [13] проведен сравнительный анализ организации информационного обмена между вычислительными модулями во встраиваемых (малых) системах реального времени на основе высокоскоростного интерфейса SRIO и межмашинного прямого доступа к памяти.

На основе алгоритмов работы интерфейса SRIO [16–17] определены временные характеристики приемо — передачи данных между конечными абонентами, объединенными посредством дуплексного звена SRIO, в различных режимах (пассивном, активном) работы интерфейса.

Следует отметить, что организация обмена данными посредством дуплексного звена SRIO не позволяет реализовать метод конвейерной передачи, что определено организацией логического уровня интерфейса SRIO.

Без учета времени оповещения конечного абонента о приеме сообщения, в режиме прерывания программы, и времени передачи ответного пакета, полное время приемо-передачи одного сообщения между двумя абонентами составит:

– для пассивного режима работы:

$$T_{\text{П-П.пас}} = 2t_{\text{ка}}(n_{\text{пр}} + 1{,}5) + 4t_{\text{А}}(NK + 0{,}25);$$

– для активного режима работы:

$$T_{\text{П-П.а}} = 2t_{\text{ка}}(N_{\text{цбо}} + 1) + 3t_{\text{ка}} + 2t_{\text{А}}(n_{\text{пр}} + 1 + 2NK);$$

В случае передачи группы сообщений, с учетом времени организации режима работы, время приема-передачи составит:

– для пассивного режима работы:

$$T_{\text{srapid-П}} = C\,[2t_{\text{ка}}(n_{\text{пр}} + 1{,}5) + 4t_{\text{А}}(NK + 0{,}25);$$

– для активного режима работы:

$$T_{\text{srapid-A}} = 2t_{\text{ка}}(N_{\text{цбо}} + 1) + C[3t_{\text{ка}} + 2t_{\text{А}}(n_{\text{пр}} + 1 + 2NK)];$$

где $t_{\text{ка}}$ — цикл шины «ввод/вывод» конечного абонента;

$t_{\text{А}}$ — время анализа данных описателя процессором адаптера, соответствует рабочему циклу «ввод — вывод» внутренней шины адаптера;

$n_{\text{пр}} \geq 3$ — количество обращений программы пользователя к рабочим адресуемым регистрам контроллеров блока сообщений;

$N_{\text{цбо}}$ — количество слов циркулярного буфера описателя;

N — количество информационных слов в сегменте;

K — количество сегментов в сообщении;

C — количество передаваемых сообщений.

Для межмашинного ПДП, реализующего способ конвейерной передачи данных между конечными абонентами, время передачи группы сообщений составит:

$$T_{\text{мпдп}} = CK\,[15t_{\text{ка}} + t_{\text{А}}(N + 1).$$

Результаты расчетов сравнения временных характеристик обмена данными при объединении конечных абонентов посредством дуплексного звена SRIO и межмашинного ПДП в различных режимах работы показаны на рисунках 7, 8, 9:

– на рис. 7 представлен режим передачи одного сообщения (C = 1), состоящего из одного пакета (K = 1) при его размере N = 8–256 (байт);

– на рис. 8 представлен режим передачи одного сообщения (C = 1), состоящего из группы пакетов, например, (K = 1–50), при N = 256 (байт);

– на рис. 9 представлен режим передачи группы сообщений, например, (C = 1–50), состоящих из группы пакетов, например, (K = 50), при их размере N = 256.

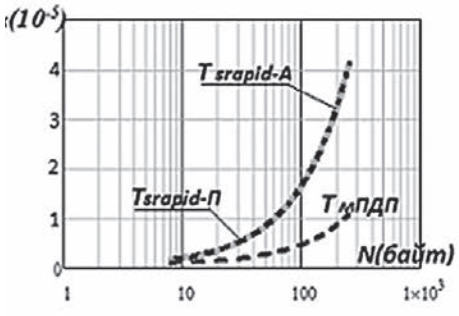


Рис. 7. Время передачи одного инф. кадра

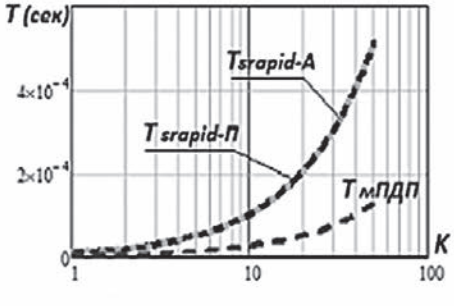


Рис. 8. Время передачи группы инф. кадра

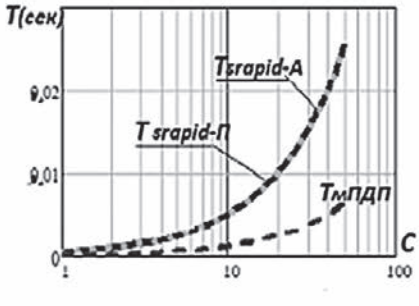


Рис. 9. Время передачи группы сообщений

Преимущество конвейерной передачи данных между конечными абонентами, реализованной на основе межмашинного ПДП, с увеличением объема передаваемых данных, растет по сравнению с использованием высокоскоростного дуплексного звена SRIO.

В работе [15] определена относительная эффективность передачи данных через адаптер дуплексного звена SRIO и адаптер межмашинного ПДП.

Относительная эффективность определяется как:

$$K_{\text{srapid-A}} = T_{\text{srapid-A}}/T_{\text{мпдп}};$$

$$KK_{\text{srapid-П}} = T_{\text{srapid-П}}/T_{\text{мпдп}};$$

Результаты расчетов представлены на рис. 10.

При увеличении объема передаваемой информации, эффективность конвейерного способа обмена данными между конечными абонентами, реализуемого посредством адаптера межмашинного ПДП, растет по отношению к реализации обмена через дуплексное звено SRIO.

Очевидно, что на время информационного обмена в реальных условиях влияют различного рода воздействия, приводящие к возникновению сбоев и соответственно к необходимости реализации повторных передач.

Среднее время обмена с учетом реализации повторных передач при возникновении сбоев составляет [9]:

1. При использовании высокоскоростного дуплексного звена SRIO:

– пассивный режим работы:

$$T_{\text{SRIO-П}} = \left[t_{\text{A}}(4N+1) + d_1\right]\sum_{i=1}^{\infty} i b_1 (1-b_1)^{i-1},$$

где $d_1 = 2t_{\text{ка}}(n + 1{,}5)$ — время организации режима работы адаптера SRIO; $b_1 = e^{-[t_{\text{A}}(4N+1)+d_1](\lambda_{\text{srio}}+\lambda_{\text{m}})}$

– вероятность бессбойной передачи;

– активный режим работы:

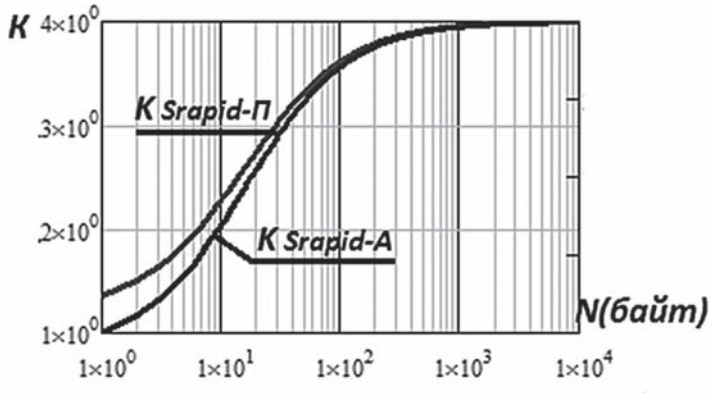


Рис. 10. Относительная эффективность способов передачи данных

$$T_{\text{SRIO-A}} = \left[2t_{\text{ка}}\left(N_{\text{цбо}}+1\right) + (3t_{\text{ка}} + d_2 + 4t_{\text{A}}N)\right]\sum_{i=1}^{\infty} i b_2 (1-b_2)^{i-1},$$

где $b_2 = e^{-[2t_{,0}(N+1)+(3t_{,0}+d_2+4t_{\text{A}}N)](\lambda_{\text{srio}}+\lambda_{\text{m}})}$. $d_2 = 2t_{\text{A}}(n+1) + 3t_{\text{ка}}$.

2. При использовании адаптера межмашинного ПДП [5]:

$$T_{\text{мпдп}} = \left[t_{\text{A}}(N+1) + d_3\right]\sum_{i=1}^{\infty} i b_3 (1-b_3)^{i-1},$$

где $d_3 = 15t_{\text{ка}}$; $b_3 = e^{-[(N+1)t_{\text{A}}+d2](\lambda_{\text{мпдп}}+\lambda_m)}$

Результаты расчетов показаны на рис. 11:

Относительная эффективность рассматриваемых способов организации обмена при возникновении сбоев определяется как (рис. 12):

$$K = T_{\text{srapid}} / T_{\text{мпдп}} \text{ (рис. 12).}$$

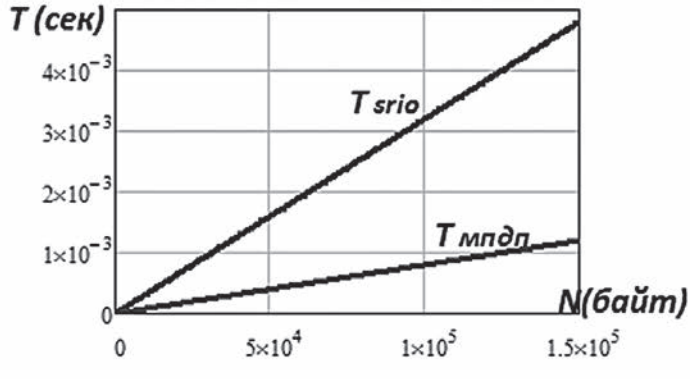


Рис. 11. Время передачи массива данных

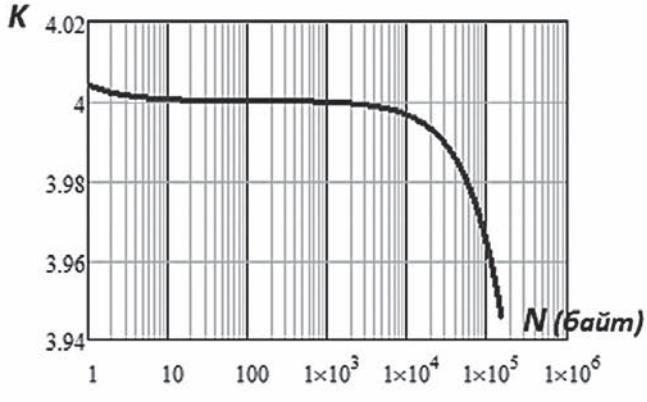
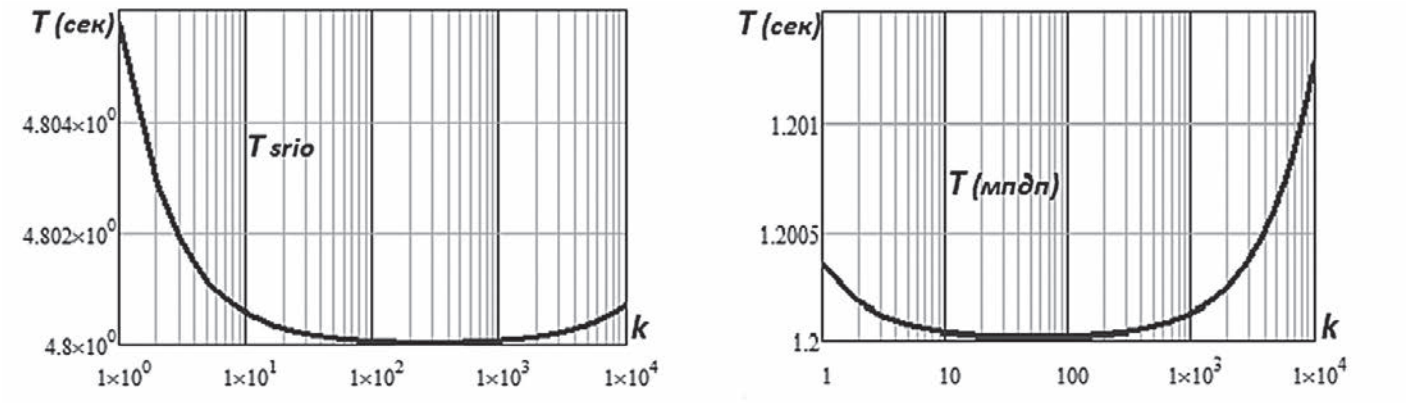


Рис. 12. Относительная эффективность обмена



а *б*

Рис. 13. Время передачи информационного массива при его разбиении на кадры

В условиях сбоев, при реализации повторных передач, сокращение времени передачи информационных массивов достигается за счет увеличения скорости при конвейерной передаче данных.

При увеличении объема передаваемой информации, в условиях сбоев, для организации информационного обмена наиболее эффективно применение межмашинного ПДП, реализующего конвейерную передачу данных.

В работе рассмотрен режим передачи информации при разбиении передаваемого массива данных на кадры.

Среднее время передаваемого массива данных, состоящего из «*N*» слов, при его разбиении на «*k*» кадров при модификации формул по [8] определяется, как:

– для организации обмена через дуплексное звено SRIO в пассивном режиме:

$$T_{\text{SRIO-П}} = (4t_{\text{A}}\frac{N}{k} + d_1)k\sum_{i=1}^{\infty} ib_1(1-b_1)^{i-1},$$

где $b_1 = e^{-(4t_{\text{A}}\frac{N}{k}+d_1)(\lambda_{\text{srio}}+\lambda_{\text{m}})}$;

– для организации обмена через дуплексное звено SRIO в активном режиме:

$$T_{\text{SRIO-A}} = \left[2t_{\text{ка}}\left(N_{\text{цбо}}+1\right) + (3t_{\text{ка}} + d_2 + 4t_{\text{A}}\frac{N}{k})k\right]\sum_{i=1}^{\infty} ib_2(1-b_2)^{i-1},$$

где $b_2 = e^{-\left[2t_{\text{ка}}(N+1)+(3t_{\text{ка}}+d_2+4t_{\text{A}}\frac{N}{k})\right](\lambda_{\text{srio}}+\lambda_{\text{m}})}$;

Результаты расчетов представлены на рис. 13а:

– для организации обмена посредством межмашинного ПДП (рис. 13б):

$$T_{\text{мпдп}} = \left[t_{\text{A}}(\frac{N}{k}+1) + d_3\right]k\sum_{i=1}^{\infty} ib_3(1-b_3)^{i-1},$$

где $b_3 = e^{-\left[\left(\frac{N}{k}+1\right)t_{\text{A}}+d_3\right](\lambda_m+\lambda_{\text{мпдп}})}$.

Расчеты произведены при N = 150 МГб; k = 1–10000.

Разбиение, передаваемого массива данных на кадры, в условиях сбоев, а значит при необходимости организации повторных передач, позволяет реализовать, для каждого из рассматриваемых способов передачи, покадровую передачу массива данных с наименьшими затратами времени.

Относительная эффективность рассмотренных способов передачи данных, при разбиении информационного массива на кадры, определяется как:

$$K_{\text{sr/пдп}} = T_{\text{srapid}}/T_{\text{мпдп}}.$$

Результаты расчетов приведены на рис. 14.

Проведенный анализ показывает, что в реальных условиях, при наличии помех, наиболее эффективна передача данных на высоких скоростях с разбиением информа-

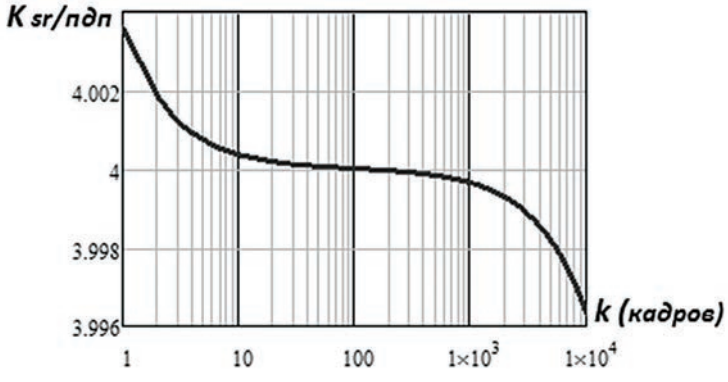


Рис. 14. Относительная эффективность обмена при разбиении информационного массива на кадры

ционного массива на кадры и организацией конвейерной передачи данных на основе межмашинного ПДП.

Разбиение на кадры позволяет реализовать устойчивую к помехам передачу данных с наименьшими затратами времени, что обеспечивает дополнительный ресурс обеспечения информационно-функциональной безопасности, надежности, в том числе при объединении вычислительных узлов и узлов хранения в системах кластерной архитектуры.

Проведенные исследования показывают, что в соответствии с принципом импортозамещения, для организации высокоскоростного информационного обмена во встраиваемых (малых) вычислительных комплексах, определяющих архитектуру магистрально-модульных БНПК наиболее эффективно применение отечественного способа организации обмена данными — межмашинного ПДП, реализующего конвейерную передачу данных, по сравнению с интерфейсом SRIO, разработанным и применяемым компаниями Texas Instruments, Freescale, Semiconductor и др.

В работе [16] проведен анализ влияния организации информационного обмена во встраиваемых системах на эффективность обеспечения восстановления вычислительного процесса (ВВП) после возникновения отказов.

Рассматриваются дублированные ВК с организацией обмена данными посредством высокоскоростного дуплексного звена SRIO и адаптера, реализующего межмашинный ПДП (мПДП).

Следует отметить, что применение высокоскоростного дуплексного звена SRIO, в отличие от реализации обмена данными посредством межмашинного ПДП, не позволяет обеспечить доступ к памяти ВМ с отказавшим процессором.

Рассматривая двухмашинные вычислительные комплексы предполагается, что время выполнения запросов является критичным. Прерванную обработку запросов необходимо восстанавливать, используя механизм КТ. Таким образом, полукомплексы регулярно обмениваются данными, необходимыми для восстановления вычислительного процесса.

Как было показано выше, время информационного обмена для рассматриваемых структур и способов организации обмена вычисляется по следующим формулам:

– для применения межмашинного ПДП:

$$T_{\text{мп дп}} = T_{\text{ор}} + t\,(N + 1),$$

где $T_{\text{ор}}$ — время организации режима работы, t — длительность цикла шины (ввод/вывод), N — количество слов информационного массива.

– для пассивного режима работы адаптера высокоскоростного дуплексного звена SRIO:

$$T_{\text{srapid-П}} = 2t_{\text{ка}}(n_{\text{пр}} + 1{,}5) + 4t_{\text{А}}(N + 0{,}25),$$

где $t_{\text{ка}}$ — длительность цикла шины (ввод/вывод) конечного абонента, $t_{\text{А}}$ — длительность цикла шины (ввод/вывод) адаптера дуплексного звена SRIO;

– для активного режима работы адаптера высокоскоростного дуплексного звена SRIO:

$$T_{\text{srapid-А}} = 2t_{\text{ка}}(N_{\text{цбо}}+1) + 3t_{\text{ка}} + 2t_{\text{А}}\,(n_{\text{пр}} + 1 + 2N),$$

где $N_{\text{цбо}}$ — количество слов циркулярного буфера описателя.

Время, затрачиваемое на пересылку данных КТ, зависит от реализации обмена данными между вычислительными модулями комплекса.

Потеря производительности комплекса, определяемая временем передачи данных КТ с учетом времени формирования (загрузки данных) КТ, составляет: $T^* = \dfrac{(t_{\text{пкт}} + t_{\text{зкт}})}{t_{\text{икт}}}$, где T^* — потеря производительности вычислительного комплекса, $t_{\text{пкт}}$ — время передачи данных КТ, определяется способом организации обмена между вычислительными модулями вычислительного комплекса, $t_{\text{зкт}} = \dfrac{8N_{\text{кт}}}{F}$ — время формирования (загрузки данных) КТ, $t_{\text{икт}}$ — интервал времени передачи данных КТ.

1. Для реализации обмена посредством высокоскоростного канала SRIO:

– для пассивного режима работы адаптера SRIO:

$$T^*_{srio-\text{П}} = \frac{8\left(1{,}5+n\right)\dfrac{1}{F_{\text{ка}}} + 4\dfrac{1}{F}(4N_{\text{кт}}+1) + \dfrac{8N_{\text{кт}}}{F}}{t_{\text{икт}}},$$

– для активного режима работы адаптера SRIO:

$$T^*_{srio-\text{А}} = \frac{8\left(1+N_{\text{цбо}}\right)\dfrac{1}{F_{\text{ка}}} + 8\dfrac{1}{F_{\text{А}}}(2N_{\text{кт}}+1+n) + 12\dfrac{1}{F_{\text{ка}}} + \dfrac{8N_{\text{кт}}}{F_{\text{ка}}}}{t_{\text{икт}}}.$$

2. Для реализации обмена посредством адаптера межмашинного ПДП:

$$T^*_{\text{мпдп}} = \frac{4\left(N_{\text{кт}}+1\right)\dfrac{1}{F_{\text{А}}} + 15\dfrac{4}{F_{\text{ка}}} + \dfrac{8N_{\text{кт}}}{F_{\text{ка}}}}{t_{\text{икт}}}.$$

Для расчета принимаем: $F_{\text{ка}}$ = 400 МГц; $F_{\text{А}}$ = 800 МГц; $N_{\text{кт}}$ = 100 Кбайт.; n = 3; $N_{\text{цбо}}$ = 1.

Результаты расчета представлены на рис. 15.

При приемлемой потере производительности $T^* = 5\%$ минимальный интервал времени передачи данных КТ составляет:

– для реализации обмена посредством высокоскоростного канала SRIO в пассивном режиме работы:

$t_{\text{srio-П}} = 0{,}08$ с;

– для реализации обмена посредством высокоскоростного канала SRIO в активном режиме работы:

$t_{\text{srio-A}} = 0{,}08$ с;

– для реализации обмена посредством адаптера межмашинного ПДП:

$t_{\text{мпдп}} = 0{,}05$ с.

Величина интервала времени передачи данных КТ ($t_{\text{икт}}$), времени взаимоконтроля ($t_{\text{вк}}$) и времени загрузки данных КТ ($t_{\text{зкт}}$) определяет возможное время восстановления вычислительного процесса ($t_{\text{ввп}}$) после отказа:

$$t_{\text{ввп}} \geq t_{\text{икт}} + t_{\text{вк}} + t_{\text{зкт}};\ \text{отсюда:}\ t_{\text{икт}} = t_{\text{ввп}} - t_{\text{вк}} - t_{\text{зкт}}.$$

Потеря производительности ВК при реализации передачи информации о КТ составит:

$$T^* = t_{\text{пкт}}/t_{\text{икт}} \text{ или } T^* = \frac{t_{\text{пкт}}}{t_{\text{ввп}} - t_{\text{вк}} - t_{\text{зкт}}}:$$

– для реализации обмена посредством высокоскоростного канала SRIO в пассивном режиме работы:

$$T^*_{\text{srio-П}} = \frac{8\left(1{,}5+n\right)\frac{1}{F_{\text{ка}}} + 4\frac{1}{F_{\text{A}}}(4N_{\text{кт}}+1)}{t_{\text{ввп}} - 8\left(1{,}5+n\right)\frac{1}{F_{\text{ка}}} - 4\frac{1}{F_{\text{A}}}(4N_{\text{вк}}+1) - 8\frac{N_{\text{кт}}}{F_{\text{ка}}}},$$

– для реализации обмена посредством высокоскоростного канала SRIO в активном режиме работы:

$$T^*_{\text{srio-A}} = \frac{8\left(1+N_{\text{цбо}}\right)\frac{1}{F_{\text{ка}}} + 2\frac{4}{F_{\text{A}}}(2N_{\text{кт}}+1+n) + 3\frac{4}{F_{\text{ка}}}}{t_{\text{ввп}} - 8\left(1+N_{\text{цбо}}\right)\frac{1}{F_{\text{ка}}} - 2\frac{4}{F_{\text{A}}}(2N_{\text{вк}}+1+n) - 3\frac{4}{F_{\text{ка}}} - 8\frac{N_{\text{кт}}}{F_{\text{ка}}}},$$

– для реализации обмена посредством адаптера межмашинного ПДП:

$$T^*_{\text{мпдп}} = \frac{4\left(N_{\text{кт}}+1\right)\frac{1}{F_{\text{A}}} + 15\frac{4}{F_{\text{ка}}}}{t_{\text{ввп}} - 8\left(N_{\text{вк}}+1\right)\frac{1}{F_{\text{A}}} - 30\frac{4}{F_{\text{ка}}} - 8\frac{N_{\text{кт}}}{F_{\text{ка}}}}.$$

Для расчета принимаем: $F_{\text{ка}} = 400$ МГц; $F_{\text{A}} = 800$ МГц; $N_{\text{кт}} = 100$ *Кбайт.;* $n = 3$; $N_{\text{цбо}} = 1$.

Результаты расчета представлены на рис. 16.

При приемлемой потере производительности $T^* = 5\%$ время восстановления вычислительного процесса (ВВП) для рассматриваемых структур составит:

– для реализации обмена посредством высокоскоростного канала SRIO в пассивном режиме работы:

$$t\ \text{ввп}_{\text{srio-П}} = 0{,}042 \text{ с};$$

– для реализации обмена посредством высокоскоростного канала SRIO в активном режиме работы:

$$t\ \text{ввп}_{\text{srio-A}} = 0{,}042 \text{ с};$$

– для реализации обмена посредством адаптера межмашинного ПДП:

$$t\ \text{ввп}_{\text{мпдп}} = 0{,}012 \text{ с}.$$

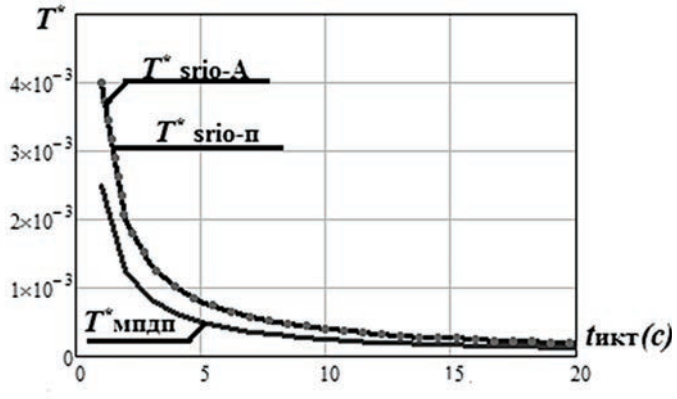


Рис. 15. Зависимость потери производительности от интервала времени передачи данных КТ

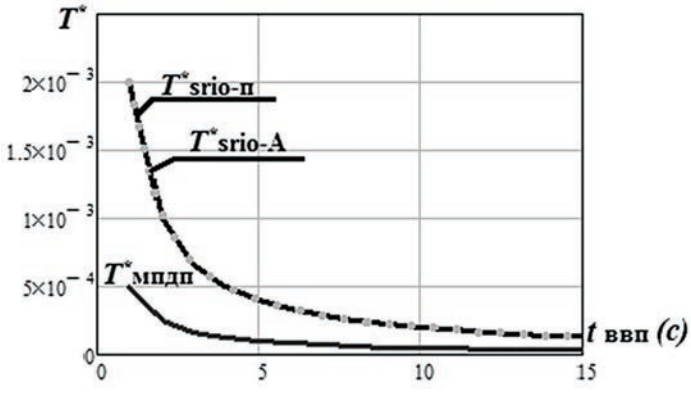


Рис. 16. Зависимость потери производительности от времени восстановления вычислительного процесса

Организация информационного обмена посредством высокоскоростного дуплексного звена SRIO характеризуется большей потерей производительности ВК, при сокращении интервала времени передачи данных КТ, а также при сокращении времени восстановления вычислительного процесса, по сравнению с организацией обмена посредством адаптера, реализующего межмашинный ПДП.

Применение, в рассматриваемых структурах БНПК, межмашинного ПДП позволяет реализовать высокоскоростной доступ к памяти вычислительного модуля с отказавшим процессором, что обеспечивает более широкие возможности доступа к данным, необходимым для восстановления вычислительного процесса, а значит, позволяет повысить живучесть вычислительного комплекса, при отказах аппаратных средств, за счет реконфигурации структуры на основе, сохранивших работоспособность модулей.

Обеспечение наименьшего времени восстановления вычислительного процесса, для рассматриваемых БНПК, возможно при организации обмена данными между вычислительными модулями комплекса на основе межмашинного ПДП.

В соответствии с принципом импортозамещения, для сокращения времени восстановления вычислительного процесса после возникновения отказа, во встраиваемых системах реального времени, наиболее эффективно применение отечественного способа организации обмена данными — межмашинного ПДП, реализующего конвейерную передачу данных, по сравнению с интерфейсом SRIO, применяемым зарубежными компаниями.

Литература

1. *Пилипенко В. Ф.* Безопасность: теория, парадигма, концепция, культура: Словарь-справочник. Изд. 2-е, доп. и перераб. М.: ПЕР СЭ-Пресс, 2005. 192 с.

2. *Богатырев В. А., Иванов Л. С., Апинян В. В.* Математическая модель мультипроцессорных систем с общей магистралью // Техника средств связи. Серия Техника проводной связи. 1985. № 4. С. 113–118.

3. *Беззубов В. Ф.* Сравнительный анализ методов обмена в многопроцессорных системах // Вестник компьютерных и информационных технологий. 2006. № 4. С. 51–56.

4. Авторское свидетельство № 1462341 G 06 F 15/16. Устройство для сопряжения ЭВМ / Беззубов В. Ф. Заявл. 01.12.1986; Опубл. 28.02.1989. Бюл. № 8. 7 с.

5. Патент РФ № 2598111. Способ управления летательным аппаратом при заходе на посадку / Криворучко Ю. Т., Пономаренко Б. В. Заявл. 30.12.2014. Опубл. 20.09.2016. 15 с.

6. *Пахолков Г. А., Збрицкая Г. Е., Криворучко Ю. Т., Пономаренко Б. В., Шатраков Ю. Г.* Обработка сигналов в радиотехнических системах ближней навигации. М.: Радио и связь, 1992. 256 с.

7. *Богатырев В. А., Беззубов В. Ф., Голубев И. Ю.* Сравнительный анализ структур отказоустойчивых дублированных вычислительных комплексов // Информационно-измерительные и управляющие системы. 2011. № 2. С. 8–12.

8. *Богатырев В. А., Голубев И. Ю., Беззубов В. Ф.* Организация межмашинного обмена в дублированных вычислительных комплексах // Известия ВУЗов. Приборостроение. 2012. № 3. С. 8–13.

9. *Беззубов В. Ф., Музелин Ю. Н.* Аппаратные средства реконфигурации структуры вычислительных комплексов // Информационно-измерительные и управляющие системы. 2015. № 12. С. 48–53.

10. Авторское свидетельство № 1798946 H 05 K 10/00, G 06 F. Резервированная вычислительная система. 11/20 / Беззубов В. Ф., Кравцов Л. Я., Эйдельсон Г. З., Гуляев А.М., Осипов Ю.И. Заявл. 09.11.89. Опубл. 28.02.93. Бюл. № 8. 8 с.

11. *Беззубов В. Ф.* Управляющая вычислительная система высокой надежности с реконфигурацией // Информационно — измерительные и управляющие системы. 2010. № 3. С. 46–50.

12. *Беззубов В. Ф., Музелин Ю. Н., Алексанков С. М., Демидов В. Д.* Использование прямого доступа к памяти для организации информационного обмена // Известия ЮФУ «Технические науки». 2014. № 12. С. 6–16.

13. *Беззубов В. Ф., Музелин Ю. Н., Турбин С. С.* Организация высокоскоростного информационного обмена во встраиваемых системах реального времени // Информационно-измерительные и управляющие системы. 2015. № 2. С. 42–49.

14. *Слепо Н.* RapidIO — коммутационная структура последовательного типа. URL: http://www.electronics.ru/journal/article/760 (дата обращения 05.10.2018).

15. Последовательный интерфейс RapidIO и его применение в пакетной коммутации. URL: http://www.russianelectronics.ru/leader-r/review/2191/doc/44291/ (дата обращения 05.10.2018).

16. *Беззубов В. Ф., Музелин Ю. Н., Турбин С. С.* Эффективность обеспечения восстановления вычислительного процесса после возникновения отказа во встраиваемых системах // Информационно-измерительные и управляющие системы. 2015. № 4. С. 22–27.

PROVIDING INFORMATION AND FUNCTIONAL SAFETY OF ANLE FOR SPECIAL PURPOSE

VLADIMIR F. BEZZUBOV
St. Petersburg, Russia, Bezzubov_vf@mail.ru

YURIY T. KRIVORUCHKO
St. Petersburg, Russia, krivoruchko.yuri@mail.ru

YURIY N. MUZELIN
St. Petersburg, Russia, yuri.muzelin@gmail.com

KEYWORDS: safety; reliability; availability; excessiveness, excess; readiness; maintainability; repairability; fail-safe feature; resiliency; airbourne navigathion and landing equipment.

ABSTRACT

The work deals with the methods for providing information and functional security of airbourne navigathion and landing equipment for special (military) purposes based on machine-to-machine direct access to memory, as well as hardware reconfiguration of the system structure in case of failure. The analysis of the organization of information exchange between computational modules in real-time systems based on RDMA Consortium technology, high-speed SRIO interface and machine-to-machine direct memory access has been carried out. It is shown that, in accordance with the principle of import substitution, the most effective way for the organization of high-speed information exchange in computing systems is to use the domestic method of organizing data exchange - a machine-to-machine direct memory access that implements conveyor data transfer compared to the RDMA Consortium technology, and the SRIO interface developed by Texas Instruments, Freescale, Semiconductor and others. The comparative analysis of the temporal characteristics of the restoration of the computational process after a failure, in real-time systems based on the RapidIO- SRIO serial interface and based on the interface of the machine-to-machine direct memory access is carried out. It is shown that, in accordance with the principle of import substitution, the most effective means to reduce the recovery time of the computational process after a failure in real-time systems compared to the SRIO interface applied by foreign companies is using of the domestic method of organizing data exchange – a machine-to-machine direct memory access realizing conveyor data transfer. The results of a comparative analysis of the use of hardware and software for organizing the restoration of the performance of airbourne navigathion and landing equipment after a failure by means of the structure reconfiguration are presented. It is demonstrated that the use of hardware control and management of the reconfiguration of the structure in combination with the machine-to-machine communication manual allows to increase the efficiency of ensuring information and functional security of airbourne navigathion and landing equipment for special (military) purposes.

REFERENCES

1. Pilipenko V. F. (Ed.).*Bezopasnost: teoriya, paradigma, koncepciya, kultura. Slovar-spravochnik* [Security: theory, paradigm, concept, culture. Dictionary-Reference]. Moscow: PER SE-Press, 2005. 192 p. (In Russian)
2. Bogatyrev V.A., Ivanov L. S., Apinyan V. V.Matematicheskaya model' mul'tiprotsessornykh sistem s obshchey magistral'yu [Mathematical model of multiprocessor systems with a common backbone]. *Tekhnika sredstv svyazi. Seria Tekhnika provodnoj svyazi* [Communications equipment]. 1985. No. 4. Pp. 113–118. (In Russian)
3. Bezzubov V. F. Sravnitel'nyy analiz metodov obmena v mnogoprotsessornykh sistemakh [Comparative analysis of exchange methods in multiprocessor systems]. *Vestnik komp'iuternykh i informatsionnykh tekhnologii* [Herald of computer and information technologies]. 2006. No. 4. Pp. 51–56. (In Russian)
4. Copyright certificate 1462341 G 06 F 15/16. *Ustroystvo dlya sopryazheniya EVM* [Device for interfacing a computer] / Bezzubov V. F. Declared 01.12.1986. Published 28.02.1989. Bulletin No. 8. 7 p. (In Russian)
5. Patent RF 2598111. *Sposob upravleniya letatel'nym apparatom pri zakhode na posadku* [Method of aircraft control during landing approach]/ Krivoruchko Yu.T., Ponomarenko B. V. Declared 30.12.2014. Published 20.09.2016. 15 p. (In Russian)
6. Pakholkov G.A., Zbritskaya G. E., Krivoruchko Yu.T., Ponoma-renko B.V., Shatrakov Yu. G. *Obrabotka signalov v radiotekhnicheskikh sistemakh blizhney navigatsii* [Signal processing in radio systems of short-range navigation]. Moscow: Radio i svyaz', 1992. 256 p. (In Russian)
7. Bogatyrev V.A., Bezzubov V. F., Golubev I. Yu. Comparative analysis of structure of the failure-safe duplicated computer complex. *Informatsionno-izmeritelnye i upravlyayushchie sistemy* [Information-measuring and Control Systems]. 2011. No. 2. Pp. 8–12. (In Russian)
8. Bogatyrev V.A., Golubev I. Yu., Bezzubov V. F. arrangement of machine-machine data exchange in backup computer complex. Izvestiya vysshikh uchebnykh zavedeniy. *Priborostroenie* [Journal of Instrument Engineering]. 2012. No. 3. Pp.8–13. (In Russian)

9. Bezzubov V.F., Muzelin Yu. N. Hardware for reconfiguration structure of computer systems. *Informatsionno-izmeritelnye i upravlyayushchie sistemy* [Information-measuring and Control Systems]. 2015. No. 12. Pp. 48–53. (In Russian)
10. Copyright certificate 1798946 H 05 K 10/00, G 06 F 11/20. *Rezervirovannaya vychislitel'naya sistema* [Redundant computing system]. Bezzubov V. F., Kravtsov L. Ya., Eydel'son A.M., Gulyaev G. Z., Osipov Yu.I. Declared 09.11.89. Published 28.02.93. Bulletin No. 8. 8 p. (In Russian)
11. Bezzubov V. F. The control system of high reliability with reconfiguration. *Informatsionno-izmeritelnye i upravlyayushchie sistemy* [Information-measuring and Control Systems]. 2010. No. 3. Pp. 46–50. (In Russian)
12. Bezzubov V.F., Muzelin Y. N., Aleksankov S. M., Demidov V. D. Application of direct memory access to the organization of information exchange. *Izvestiya SFedU*. [Engineering Sciences]. 2014. No. 12. Pp. 6–16. (In Russian)
13. Bezzubov V.F., Muzelin Yu.N., Turbin S. S. Organization of high-speed information exchange in embedded real-time systems. *Informatsionno-izmeritelnye i upravlyayushchie sistemy* [Information-measuring and Control Systems]. 2015. No. 2. Pp. 42–49. (In Russian)
14. Slepov N. R*apidIO – kommutatsionnaya struktura posledovatel'nogo tipa* [RapidIO – switching structure of the sequential type]. URL: http://www.electronics.ru/journal/article/760 (date of access 05.10.2018). (In Russian)
15. *Posledovatel'nyy interfeys RapidIO i ego primenenie v paketnoy kommutatsii* [RapidIO serial interface and its application in packet switching]. URL: http://www.russianelectronics.ru/leader-r/review/2191/doc/44291/ (date of access 05.10.2018). (In Russian)
16. Bezzubov V.F., Muzelin Yu.N., Turbin S. S.Efficiency of providing the recovery of computational process after a fault in embedded systems. *Informatsionno-izmeritelnye i upravlyayushchie sistemy* [Information-measuring and Control Systems]. 2015. No. 4. Pp. 22–27. (In Russian)

INFORMATION ABOUT AUTHORS:
Bezzubov V.F., PhD, Senior Research Officer, Federal Scientific Production Center All-Russian scientific Research Institute of Radio Equipment awarded with the Order of Red Banner (JSC "VNIIRA");
Krivoruchko Y.T., PhD, head of sector of the Federal Scientific Production Center All-Russian scientific Research Institute of Radio Equipment awarded with the Order of Red Banner (JSC "VNIIRA");
Muzelin Y.N., PhD, head of department of the Federal Scientific Production Center All-Russian scientific Research Institute of Radio Equipment awarded with the Order of Red Banner (JSC "VNIIRA")".

For citation: Bezzubov V.F., Krivoruchko Y.T., Muzelin Y.N. Providing information and functional safety of anle for special purpose. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 4–18. doi: 10.24411/2409-5419-2018-10183 (In Russian)

doi: 10.24411/2409-5419-2018-10184

АНАЛИЗ ЛИНИИ ПЕРЕДАЧИ ДАННЫХ АВТОМАТИЧЕСКОГО ЗАВИСИМОГО НАБЛЮДЕНИЯ ВЕЩАТЕЛЬНОГО ТИПА

РУБЦОВ
Евгений Андреевич[1]

КАЛИНЦЕВ
Андрей Сергеевич[2]

ГРИГОРЬЕВА
Елена Ивановна[3]

АННОТАЦИЯ

Прогнозирование потенциальных конфликтных ситуаций, как основная функция автоматизированных систем управления воздушным движением, производится на основе анализа данных, полученных от систем авиационного наблюдения, наиболее перспективным из которых является автоматическое зависимое наблюдение. Анализ эксплуатационных характеристик этого типа наблюдения показал, что на современном этапе не удается обеспечить соблюдение требуемых характеристик: точности определения местоположения воздушных судов и надежности передачи сообщений по линиям передачи данных. В работе производится анализ линии передачи данных, применяемой для обмена информацией между воздушным судном и наземной станцией автоматического зависимого наблюдения, а также между воздушными судами по линии «борт-борт», совершающими полет по воздушной трассе. Установлено, что неоптимальная форма диаграммы направленности бортовой антенны может привести к уменьшению дальности действия до величины ниже требуемой. Для класса оборудования А2 эксплуатационная дальность составит 42 км при требуемой 74 км, для класса оборудования А3 эксплуатационная дальность составит 85 км при требуемой 167 км. Эти особенности необходимо учитывать. Также рекомендуется внедрить антенны, диаграммы направленности которых не имеют ярко выраженных минимумов. Также рассмотрены такие недостатки, как отсутствие помехоустойчивого кодирования и механизмов защиты информации передаваемого сообщения. Рассмотрены возможные пути устранения этих недостатков, которые позволят ужесточить требования по допустимому отношению количества ошибочных сообщений к общему числу переданных (в настоящее время отношение 1 к 105). Рекомендуется применять более совершенные методы помехоустойчивого кодирования. При этом отмечен такой негативный момент, как уменьшение информационной емкости сообщения, что приводит к необходимости его передачи несколькими пакетами и увеличении нагрузки на линию. Для уменьшения уязвимости предлагается ввести режим «закрытой передачи», при котором вводится шифрование сообщений. Это потребует принятия дополнительных нормативных документов, устанавливающих правила шифрования и условия введения такого режима.

КЛЮЧЕВЫЕ СЛОВА: автоматизированная система управления воздушным движением; безопасность полетов; автоматическое зависимое наблюдение; линия передачи данных; диаграмма направленности антенны; помехоустойчивое кодирование.

Сведения об авторах:
[1]к.т.н., доцент кафедры радиоэлектронных систем Санкт-Петербургского государственного университета гражданской авиации, г. Санкт-Петербург, Россия, Rubtsov.spb.guga@rambler.ru

[2]соискатель кафедры радиоэлектронных систем Санкт-Петербургского государственного университета гражданской авиации, г. Санкт-Петербург, Россия, Kas4job@gmail.com

[3]старший преподаватель кафедры радиоэлектронных систем Санкт-Петербургского государственного университета гражданской авиации, г. Санкт-Петербург, Россия, 25_Grig@mail.ru

Для цитирования: *Рубцов Е.А., Калинцев А.С., Григорьева Е.И.* Анализ линии передачи данных автоматического зависимого наблюдения вещательного типа // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 19–27. doi: 10.24411/2409-5419-2018-10184

В основе современных автоматизированных систем управления воздушным движением (АС УВД) лежит принцип обеспечения требуемого уровня безопасности полетов, путем выдерживания воздушными судами (ВС) интервалов горизонтального и вертикального эшелонирования. Мониторинг состояния воздушного пространства предполагает определение местоположения ВС с точностью, достаточной для прогнозирования потенциальных конфликтных ситуаций, для чего используются разнообразные средства авиационного наблюдения [1–3].

До недавнего времени магистральным направлением развития авиационного наблюдения являлось внедрение автоматического зависимого наблюдения (АЗН). В частности, планировалось обеспечить перекрытие воздушного пространства России полем вещательного АЗН (АЗН-В), что обеспечило бы значительную экономическую выгоду по сравнению с вариантом обеспечения перекрытия воздушного пространства страны средствами вторичной радиолокации. Однако, анализ эксплуатационных характеристик АЗН-В (точности, надежности) показал, что эта перспективная технология не может обеспечить соблюдение требуемых характеристик наблюдения. Данный факт отражен в документе ИКАО Doc.9924 «Руководство по авиационному наблюдению».

Рассмотрим подробнее основные характеристики автоматического зависимого наблюдения. В настоящее время существуют три технологии реализации АЗН-В, прошедшие процедуру международной стандартизации, рекомендованные ИКАО: радиолокационные самолётные ответчики, работающие в режиме S с произвольным протоколом радиовещания (1090*ES*), ОВЧ линии цифровой связи четвертого режима (*VDL*-4), использующем самоорганизующийся протокол с разделением во времени и приемопередатчики универсального доступа (*UAT*) [3–4]. С2003 года Аэронавигационная конференция ИКАО рекомендует применять технологию 1090ES в качестве глобального решения для реализации АЗН-В.

В США для обеспечения полетов авиации общего назначения, ВС региональных авиалиний и частных полетов применяется *UAT*, а для обеспечения полетов магистральных ВС — 1090ES. В России также планировалось применять две линии передачи данных: *VDL*-4 и 1090ES, однако с 2017 года решением Росавиации было утверждено применение линии 1090ES для гражданских ВС всех типов.

При внедрении АЗН-В, наблюдение за воздушным движением будет осуществляться как с помощью перспективных методов, так и с использованием традиционных радиолокационных средств. Во время переходного периода воздушные суда, оснащенные оборудованием АЗН-В, не будут получать полной информации об окружающей их воздушной обстановке в части неоснащенных воздушных судов. Это существенно снизит эффективность использования системы АЗН-В в целях поддержки бортовых функций наблюдения. Чтобы улучшить ситуацию, необходимо обеспечивать вместе с АЗН-В услугу информирования экипажей об окружающей воздушной обстановке по линии передачи данных «Земля-борт» (услуга *TIS-B*). *TIS-B* использует информацию от наземных систем наблюдения, например, радиолокационных систем, и в радиовещательном режиме осуществляет передачу этой информации на борт ВС. Как правило, для *TIS-B* и АЗН-В используется единая линия передачи данных, однако для *TIS-B* применяются другие форматы сообщений, отличные от АЗН-В [5–6].

Согласно программе «Внедрение средств вещательного автоматического зависимого наблюдения (2011–2020 годы)», утвержденной Минтрансом России 19.05.11, необходимо обеспечить глубокую модернизацию систем наблюдения единой системы организации воздушного движения (ЕС ОрВД) на основе внедрения инновационных технологий АЗН-В, функционирующего на основе информации глобальных навигационных систем ГЛОНАСС/*GPS* и предназначенного для использования в интересах обслуживания воздушного движения и мониторинга воздушных судов. Задачи программы включают:

– проведение исследований с целью уточнения технической архитектуры АЗН-В для реализации в ЕС ОрВД России;

– оснащение аэродромов наземными станциями АЗН-В;

– размещение дополнительных средств АЗН-В и поддерживающих систем для обеспечения потребностей пользователей в нижнем воздушном пространстве;

– разработка требуемых бортовых компонент АЗН-В;

– разработка нормативных правовых документов, обеспечивающих использование систем АЗН-В в целях организации воздушного движения;

– обеспечение перехода к современным технологиям организации воздушного движения, основанным на внедрении средств АЗН-В.

На начальном этапе внедрения АЗН-В в России были реализованы три пилотных проекта: «Москва-АЗН», «Балтика-АЗН» и «Ямал-АЗН». На базе пилотных проектов в настоящее время развиваются региональные проекты, суть которых заключается в наращивании наземной инфраструктуры станций АЗН-В, а также оборудование воздушных судов необходимой аппаратурой. Для перехода на режим *S* необходимо оснащение всех воздушных судов ответчиками этого режима. Такая работа была уже проведена в Европе. Опыт наблюдения за воздушным пространством над Санкт-Петербургом показал, что практически 100% воздушных судов гражданской авиации уже

оборудованы ответчиками режима *S*, из них около 80% имеют возможности передавать информацию АЗН-В в режиме 1090*ES*. Дальнейшее развитие технологии АЗН-В предполагает перекрытие воздушного пространства полем систем наблюдения в масштабе всей страны [3].

Проведем анализ характеристик линии передачи данных 1090*ES*. Технология 1090*ES* имеет широкий спектр использования [3–7]:

– наземное наблюдение в целях управления воздушным движением с высокой целостностью;

– обеспечение пользователей воздушного пространства возможностью полетов в разные регионы мира (глобальная совместимость бортового и наземного оборудования 1090*ES*);

– наземное наблюдение с использованием технологий мультилатерации;

– режимы передачи закрытой информации для государственных организаций.

К основным характеристикам технологии 1090ES относятся:

– битовая скорость передачи информации — 1 Мбит/с;

– эффективная скорость передачи пользовательской информации — 200–300 кбит/с;

– выделенный частотный диапазон (глобально для всех регионов мира);

– установленные на ВС фидерные системы, не требующие дополнительной модификации;

– сопрягаемость с технологией вторичной радиолокации и бортовой системой предупреждения столкновений (*TCAS/ACAS*).

Сообщение АЗН-В, передаваемое с борта ВС включает [1, 6–7]:

– опознавательный индекс воздушного судна;

– местоположение ВС;

– скорость ВС;

– намерение изменить траекторию.

Сообщение состоит из преамбулы и блока данных. Преамбула представляет собой последовательность из четырех импульсов, а блок данных — последовательность импульсов с двоичной времяимпульсной модуляцией. Объем сообщения составляет 112 бит, длительность — 120 микросекунд. В среднем может излучаться ежесекундно 6,2 сообщений [6].

Сообщение состоит из двух полей. Первое описывает формат и содержит адрес ответчика. За исключением форматов удлиненных сообщений, дескриптором, т.е. полем, описывающим формат, является пяти битовое поле, с которого начинается передача, а адресное поле, объемом 24 бита, всегда располагается в конце сообщения. Поле адреса содержит либо адрес ответчика, либо идентификатор системы вторичной радиолокации, наложенный на проверочную информацию (контроль целостности). В этом случае сообщение может содержать до 56 бит информации [3, 6].

Форматы удлиненных сообщений (с объемом информационной части 80 бит) определяются первыми двумя битами блока данных, при этом в обоих битах устанавливают единицу. Таким образом, для передачи удлиненных сообщений выделяют коды форматов с 24 по 31 [3, 6].

В запросах и ответах режима *S* используют кодирование с проверкой на четность, которое обеспечивает защиту от воздействия помех. Последовательность из 24 проверочных битов помещается в поле, образованное последними 24 битами всех передач режима *S*. При этом 24 проверочных бита объединяют либо с адресным кодом, либо с кодом идентификатора запросчика. В результате образуется либо поле «адрес/проверка», либо поле «проверка/идентификатор запросчика» [3, 6].

Последовательность из 24 проверочных битов (*P*1, *P*2, …, *P*24) образуется с помощью последовательности информационных битов (*M*l, *M*2, …, *MK*), где К равно 32 или 88 для коротких или длинных передач соответственно. Для этой цели используют код, выраженный многочленом [3, 6]:

$$G(X) = 1 + X^3 + X^{10} + X^{12} + X^{13} + \\ + X^{14} + X^{15} + X^{16} + + X^{17} + X^{18} + X^{19} + \\ + X^{20} + X^{21} + X^{22} + X^{23} + X^{24} \quad (1)$$

Выражая последовательность информационных символов в виде:

$$M(X) = M_k + M_{k-1}X + M_{k\square 2}X^2 + \ldots + M_i X^{k-1} \quad (2)$$

и разделив этот многочлен по правилам двоичной алгебры многочленов на многочлен *G*(*X*), в результате получим некоторое частное и остаток *R*(*X*), степень которого менее 24. Последовательность битов, образованная этим остатком, составляет последовательность проверочных сигналов. При этом бит P_i, для любого *i* от 1 до 24 равен коэффициенту при X^{24-i} в *R*(*X*) [3, 6].

Бортовое оборудование АЗН-В, использующее линию 1090ES принято делить на 4 класса: *A*0, *A*1, *A*2 и *A*3. Оборудование класса А0 является минимально необходимым, применяется только по правилам визуальных полетов (ПВП). Оборудование классов *A*1–*A*3 применяется по правилам полетов по приборам (ППП), при этом *A*1 является базовым, *A*2 — усовершенствованным. *A*3 — расширенным. Классы бортового оборудования АЗН-В и их характеристики приведены в табл. 1 [1, 8–9].

Таблица 1

Характеристики бортового оборудования АЗН-В 1090*ES*

Класс оборудования	Максимальная мощность передачи, дБВт	Минимальный пороговый уровень приемника, дБмВт
A0	18,5	– 72
A1	21,0	– 79
A2	21,0	– 79
A3	23,0	– 84

Анализ табл. 1 позволяет определить требуемое значение мощности передатчика и минимальный уровень сигнала на входе приемника. В табл. 2 приведены теоретически достижимые значения дальности действия оборудования АЗН-В для различных сочетаний разных классов [1, 8–9].

Таблица 2

Дальность действия бортового оборудования АЗН-В 1090ES по линии «борт–борт»

Классы оборудования	Дальность действия по линии «борт–борт», км
A0 – A0	18
A1 – A1	37
A2 – A2	74
A3 – A3	167

Оценим дальность действия оборудования АЗН-В по линии «борт–борт». При расчетах будем учитывать потери на распространение, приведенные в рекомендации Международного союза электросвязи и телеграфии (МСЭ-Т) Р. 528 «Кривые распространения радиоволн для воздушной подвижной и радионавигационной служб, работающих в диапазонах ОВЧ, УВЧ и СВЧ». Также в расчетах учитывались диаграммы направленности бортовых антенн, полученные путем натурного моделирования (отчет FAA-RD-75–23 лаборатории Линкольна Массачусетского технологического института от 4 апреля 1975 г.). Сам расчет будет проводиться по стандартной методике для высокоподнятых антенн [10, 11].

Энергетический запас (превышение мощности передатчика над мощностью потерь) для 95% и 50% времени, рассчитывается по формулам:

$$R(0{,}95) = R(0{,}50) + Y_R(0{,}95) \qquad (3)$$

$$R(0{,}50) = P_t + G_t + G_r - L_b(0{,}95) \qquad (4)$$

$$Y_R = -\sqrt{[L_b(0.95) - L_b(0.50)]^2_{Wanted} + [L_b(0.05) - L_b(0.50)]^2_{Unwanted}} \qquad (5)$$

где P_t — мощность передатчика;

G_t, G_r — КНД передающей и приемной антенны.

Было произведено две серии расчетов. В первой серии углы крена и тангажа не превышали ±5°, при этом направление излучение и приема приходилось на максимум диаграмм направленности антенн. Во второй серии углы крена достигали ±20°, углы тангажа ±10°, при этом направление излучение и приема приходилось на минимум диаграмм направленности антенн. Результаты расчетов приведены в табл. 3.

Таблица 3

Результаты расчетов дальности действия бортового оборудования АЗН-В 1090ES

Классы оборудования	Результаты первой серии расчетов, км	Результаты второй серии расчетов, км
*A*0 – *A*0	56	39
*A*1 – *A*1	98	42
*A*2 – *A*2	98	42
*A*3 – *A*3	174	85

Анализ результатов расчета показал, что за счет неравномерной диаграммы направленности бортовых антенн, дальности действия для оборудования классов *A*2 и *A*3 окажутся меньше требуемых на 43% и 49% соответственно.

Оценим дальность действия оборудования при наличии помех. Расчет будет проводится по методике анализа радиоканалов с помехами, при передаче сигналов с двухпозиционной фазовой манипуляцией (*BPSK*) [12–13].

Введем следующие значения шумовой температуры: 10000 К, 20000 К и 30000 К для «слабой», «средней» и «сильной» помехи. Согласно спецификации 1090ES допускается прием одного неправильного сообщения на 105 переданных, таким образом вероятность приема неправильного сообщения не должна превышать $9{,}5 \cdot 10^{-3}$[9].

Вероятность ошибки приема неправильного сообщения зависит от вероятности ошибки на один бит информации (bit error rate — *BER*) [12]:

$$P_{\Pi} = 1 - \prod_{i=1}^{S}(1 - P_{Ci}) = 1 - \prod_{i=1}^{112}(1 - P_{Ci}). \qquad (6)$$

Для обеспечения требуемой вероятности приема ошибочного сообщения необходимо обеспечить вероятность ошибки на бит $8.5 \cdot 10^{-5}$.

В канале 1090ES используется двухпозиционная фазовая манипуляция (*BPSK*). Вероятность ошибки на бит находится как [12–13]:

$$P_{\text{ОШ}} = \frac{1}{2} erfc\left(\sqrt{\frac{E}{N}}\right), \quad (7)$$

где E/N — отношение сигнал/шум на выходе приемника.

Расчет радиуса рабочей области сводится к определению отношения сигнал/шум и вероятности ошибки на бит с учетом помеховой обстановки. Дальность, на которой будет обеспечена вероятность приема неправильного сообщения не более $8{,}5 \cdot 10^{-5}$ и будет рабочей областью. Для обеспечения такой вероятности необходимо, чтобы отношение сигнал/шум на выходе приемника было не менее 9 дБ [14–15].

При передаче данных применяют помехоустойчивое кодирование, однако канал 1090ES не предусматривает применения исправляющих кодов. Это означает, что повреждение одного информационного бита делает сообщение ошибочным. Данный факт отчасти компенсируется величиной требуемой вероятности приема неправильного сообщения. Таким образом, обеспечить требуемую дальность действия можно только путем увеличения отношения сигнал/шум на выходе приемника, от которого зависит вероятность ошибки на бит.

Бортовой ответчик имеет мощность, соответствующую его классу (см. табл. 1). Анализ литературы по бортовым антеннам показал, что бортовые антенны могут как усиливать сигнал до 1 дБ, так и вносить ослабление до –5 дБ вследствие формы диаграмм направленности [16].

Мощность сигнала в точке приема находится как разность мощности передатчика и потерь на распространение. Действующая длина бортовой антенны составляет 0,2…0,3 м. Исходя из этого, можно определить напряжение сигнала на входе приемника. Также необходимо знать напряжение шума. Оно складывается из собственного шума приемника и атмосферных шумов (включающих естественные и искусственные). Собственный шум приемника находится как:

$$T_{\text{ПР}} = (\text{К}_{\text{Ш ПР}} - 1) \cdot T_0, \quad (8)$$

где $K_{\text{ШПР}}$ — коэффициент шума приемника,

$T_0 = 293$ К,

При коэффициенте шума равном 10, получим:

$$T_{\text{ПР}} = (10–1) \cdot 293 = 2630 \text{ К} \quad (9)$$

Необходимо также учитывать шумовую температуру антенны $T_{\text{А}}$. Мощность шума антенны находится как:

$$P_{\text{Ш\_ПРМ}} = k(T_{\text{ПР}} + T_{\text{А}}) \cdot \Delta F, \quad (10)$$

где $k = 1{,}38 \cdot 10^{-23}$ — постоянная Больцмана,

ΔF — ширина полосы пропускания приемника.

Шумовую температуру бортовой антенны примем за 2000 К. Ширина полосы пропускания приемника 1090*ES* составляет 5 МГц. Тогда, $P_{\text{Ш\_ПРМ}} = 69 \cdot 10^{-18}$ Вт.

Мощность атмосферных шумов зависит от района, над которым совершается полет, времени суток, грозовой активности и многих других факторов, учет которых является сложной, а подчас и просто невыполнимой задачей. Поэтому, в расчетах рекомендуется применять средние значения атмосферных шумов, характерные для данного региона.

Шумовую температуру для населенной местности на частоте 1000 МГц о примем 20000 К («средняя» помеха). Тогда мощность шума составит $P_{\text{Ш\_атм}} = 71 \cdot 10^{-18}$ Вт.

Напряжение помехи, образованной суммой внутренних шумов приемника, шума антенны и атмосферного шума находится как:

$$U_{\text{П}} = \sqrt{\frac{P_{\text{Ш\_ПРМ}} + P_{\text{Ш\_арм}}}{R}} = \sqrt{\frac{69 \cdot 10^{-18} + 71 \cdot 10^{-18}}{50}} = 2{,}78 \cdot 10^{-9} \text{ В} \quad (11)$$

При повышении шумовой температуры помехи до 30000 К («сильная» помеха), напряжение помехи на выходе приемника составит $5 \cdot 10^{-9}$ В. «Слабая» помеха, имеющая шумовую температуру 10000 К, создает напряжение на выходе приемника $1 \cdot 10^{-9}$ В.

Результаты расчета дальности действия при наличии помех:

– дальность действия при наличии «слабой» помехи составит 45–50 км;

– дальность действия при наличии «средней» помехи составит 25–35 км;

– дальность действия при наличии «сильной» помехи составит 15–25 км.

Анализ результатов показывает, что при наличии даже сравнительно слабых помех (с шумовой температурой 10000 К), дальность действия будет обеспечена только для оборудования классов *A*0 и *A*1. Для оборудования классов *A*2 и *A*3 требуемая дальность обеспечена не будет. Следует обратить внимание, что наличие сильных помех (в том числе преднамеренных) может значительно ограничить дальность действия оборудования и вызвать определенные проблемы при оценке экипажем воздушной обстановки.

Решение указанных проблем должно иметь комплексный характер, однако можно выделить общие направления, по которым целесообразно проводить работы. Прежде всего необходимо обеспечить более равномерные

диаграммы направленности бортовых антенн, что позволит исключить ослабление сигнала при невыгодных сочетаниях крена и тангажа обменивающихся сообщениями воздушных судов. Также целесообразно повысить максимальную мощность бортовых передатчиков, что позволит увеличить отношение сигнал/шум на выходе приемника и уменьшить вероятность ошибки на бит (*BER*). Одним из важнейших шагов по обеспечению требуемой дальности действия в условиях наличия помех является применение более совершенных методов помехоустойчивого кодирования, в том числе исправляющих кодов (например, кода Рида-Соломона) [17–18]. При этом следует учитывать малую информационную емкость сообщения 1090ES. Это приводит к необходимости поиска компромисса между эффективностью кода (достигаемой помехоустойчивостью) и количеством пакетов, необходимых для передачи того или иного объема информации.

Одной из проблем линии 1090ES является ее открытость к внешним воздействиям. Обладая необходимой аппаратурой несанкционированный пользователь может сформировать сообщение как для бортового оборудования, так и для наземной станции АЗН-В, тем самым создав сложности и для экипажа ВС и для диспетчера управления воздушным движением [19–21]. Вопросы шифрования данных в настоящее время обсуждаются, однако единое мнение все еще не сформировано. В качестве решения можно предложить внедрение специального режима «закрытой передачи». Суть его сводится к тому, что в случае возникновения подозрения на наличие в эфире сигналов злоумышленников экипажи по команде диспетчера на определенное время переходят к передаче зашифрованных сообщений АЗН-В.

Литература

1. *Ахмедов Р. М., Бибутов А. А., Васильев А. В*. Автоматизированные системы управления воздушным движением. Новые информационные технологии в авиации / под ред. С. Г. Пятко и А. И. Красова. СПб.: Политехника, 2004. 446 с.

2. *Бестугин А. Р*. Автоматизированные системы управления воздушным движением. СПб.: Политехника, 2014. 450 с.

3. *Кудряков С. А., Кульчицкий В. К., Поваренкин Н. В., Пономарев В. В., Рубцов Е. А., Соболев Е. В., Сушкевич Б. А*. Радиотехническое обеспечение полетов воздушных судов и авиационная электросвязь. СПб.: Свое издательство, 2016. 287 с.

4. *Li T., Sun Q., Li J.* A Research on the Applicability of ADS-B Data Links in Near Space Environment // International Conference on Connected Vehicles and Expo (ICCVE2012) (Beijing, 12–16 December 2012). IEEE, 2012. Pp. 1–5. doi:10.1109/ICCVE.2012.9

5. *Ali B. S.* System specifications for developing an Automatic Dependent Surveillance-Broadcast (ADS-B) monitoring system // International Journal of Critical Infrastructure Protection. 2016. No. 15. Pp. 40–46.

6. *Воскребенцев Н. А., Рубцов Е. А*. Анализ структуры сообщения автоматического зависимого наблюдения по линии передачи данных 1090ES // Материалы Международной научно-практической конференции «Наука сегодня: проблемы и пути решения» (Вологда, 29 марта 2017 г.). Вологда: Маркер, 2017. С. 22–23.

7. *Langejan T. P., Sunil E., Ellerbroek J., Hoekstra, J. M*. Effect of ADS-B Characteristics on Airborne Conflict Detection and Resolution // 6 th SESAR Innovation: Inspiring long-term research in the field of Air Traffic Management (Netherlands, 8–10 November 2016). SESAR, 2016. Pp.1–8. https://www.sesarju.eu/sites/default/files/documents/sid/2016/SIDs_2016_paper_22.pdf (дата обращения 05.10.2018).

8. *Reck C., Reuther M. S., Jasch A., Schmidt L. P*. Independent surveillance broadcast ADS-B receivers with DOA estimation // Digital Communications — Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV). IEEE, 2011. Pp. 219–222.

9. *Stacey D.* Aeronautical radio communication systems and networks. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2008. 373 p.

10. *Вычугжанин В. Б., Рубцов Д. В*. Метод расчета статистических характеристик линии передачи данных в системах УВД с автоматическим зависимым наблюдением // Научный вестник МГТУ ГА. 2006. № 107. С. 165–169.

11. *Seybold J. S*. Introduction to RF propagation. New Jersey, Wiley-Interscience, 2005. 352 p.

12 *Simon M. K., Alouinii M.-S.* Digital Communication Over Fading Channels: A Unified Approach to Performance Analysis. New York, Wiley, 2000. 544 p.

13. *Naganawa J., Miyazaki H., Tajima H.* Measurement-Based Evaluation on Detection Probability of Extended Squitter for Air-to-Ground Surveillance // Vehicular Technology IEEE Transactions. 2017. Vol. 66. No. 10. Pp. 8883–8894.

14. *Затучный Д. А., Логвин А. И*. Определение оптимального количества линий передачи данных для реализации режима автоматического зависимого наблюдения // Научный вестник МГТУ ГА. 2013. № 189. С. 9–13.

15. *Затучный Д. А*. Повышение точности оценки достоверности информации, передаваемой при автоматическом зависимом наблюдении, на основе анализа качества дополнительных данных // Надежность и качество сложных систем. 2017. № 1. С. 11–16.

16. *Нечаев Е. Е., Будыкин Ю. А*. Антенные устройства в гражданской авиации. Курск: Пресс-факт, 2005. 380 с.

17. *Zhang Z.* Optimization performance analysis of 1090ES ADS-B signal separation algorithm based on PCA and

ICA // International Journal of Performability Engineering. 2018. Vol. 14. No. 4. Pp. 741–750.

18. *Кузьмин Б. И.* Авиационная цифровая электросвязь в условиях реализации «Концепции ИКАО-ИАТА CNS/ATM» в Российской Федерации. СПб., Н. Новгород: ВиТ-принт, 2007. 384 с.

19. *Schafer M., Lenders V., Martinovic I.* Experimental Analysis of Attacks on Next Generation Air Traffic Communication // Applied Cryptography and Network Security. 2013. Pp. 253–271.

20. *McCallie D., Butts J., Mills R.* Security analysis of the ADS-B implementation in the next generation air transportation system // International Journal of Critical Infrastructure Protection. 2011. Vol. 4. No. 2. Pp. 78–87.

21. *Leonardi M., Piracci E., Galati G.* ADS-B vulnerability to low cost jammers: risk assessment and possible solutions // Tyrrhenian International Workshop on Digital Communications — Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV). IEEE, 2014. Pp. 41–46.

DATA LINK ANALYSIS OF AUTOMATIC DEPENDENT SURVEILLANCE – BROADCAST

EVGENY A. RUBTSOV
St-Peterburg, Russia, Rubtsov.spb.guga@rambler.ru

ANDREY S. KALINTSEV
St-Peterburg, Russia, Kas4job@gmail.com

ELENA I. GRIGOREVA
St-Peterburg, Russia, 25_Grig@mail.ru

KEYWORDS: automated air traffic control system; flight safety; automatic dependent surveillance; data link; radiation pattern; error-correcting coding.

ABSTRACT

Forecasting of potential conflict situations, as the main function of automated air traffic control systems, is based on the analysis of surveillance systems data, and the most promising of them is automatic dependent surveillance. Analysis of the characteristics of this type of surveillance showed that at the present stage it's not possible to ensure compliance with the required characteristics: accuracy of aircraft location and the reliability of message transmission over data links. The work analyzes the data link used for the exchange of messages between the aircraft and the ground station of automatic dependent surveillance, as well as between the aircraft on the link "aircraft-to-aircraft", flying on the route. It is established that the non-optimal form of the radiation pattern of the aircraft antenna can lead to a reduction in the range to a value below the required one. For the A2 equipment class, the operational range will be 42 km while the required is 74 km, for the A3 equipment class the operational range will be 85 while the required is 167 km. These features must be taken into account. It is also recommended to introduce antennas, the radiation patterns of which do not have great minima. Also, consider the disadvantages such as the lack of error-correcting coding and information security mechanisms of the message transmitted. The possible ways to eliminate these shortcomings, which will strengthen the requirements for the permissible ratio of the number of error messages to the total number of transmitted (currently ratio is 1 to 105). It is recommended to use advanced methods of error-correcting coding. At the same time, such a negative moment as a decrease in the information capacity of the message is noted, which leads to the need for its transmission by several packets and an increase the link load. To reduce the vulnerability of link, it is proposed to introduce a "closed transmission" mode, in which encryption of messages is introduced. This will require the adoption of additional regulations establishing encryption rules and conditions for the introduction of such a regime.

REFERENCES

1. Achmedov P.M., Bibutov A.A., Vasiliev A.V. *Avtomatizirovannie sistemi upravlenia vozdushnim dvijeniem. Novie informacionnie technologii v aviacii: uchebnoe posobie* [Automated air traffic control systems. New information technologies in aviation: textbook]. Edited by S.G. Pyatko and A.I. Crasov. St. Petersburgb.: Politechnica, 2004. 446 p. (In Russian)

2. Bestugin A.R. *Avtomatizirovannie sistemi upravlenia vozdushnim dvijeniem: uchebnoe posobie* [Automated air traffic control systems: textbook]. St. Petesburg: Politechnica, 2014. 450 p. (In Russian)

3. Kudryakov S.A., Kulchickii V.K., Povarenkin N.V., Ponomarev V.V., Rubtsov E.A., Sobolev E.V., Sushkevitch B.A. *Radiotechnicheskoe obespechenie polyotov vozdushnih sudov i aviacionnaya electrosvyaz. Uchebnoe posobie* [Radio engineering support of aircraft flights and aviation telecommunication]. St. Petesburg: Svoe izdatelstvo, 2016. 287 p. (In Russian)

4. Li T., Sun Q., Li J. A Research on the Applicability of ADS-B Data Links in Near Space Environment. *International Conference on Connected Vehicles and Expo (ICCVE)*. Beijing, 2012. Pp. 1–5.

5. Ali B.S. System specifications for developing an Automatic Dependent Surveillance-Broadcast (ADS-B) monitoring system. *International Journal of Critical Infrastructure Protection*. 2016. No. 15. Pp. 40–46.

6. Voscrebencev N.A., Rubtsov E.A. Analiz struktury soobshcheniya avtomaticheskogo zavisimogo nablyudeniya po linii peredachi dannykh 1090ES. [Analysis of automatic dependent surveillance message structure for the 1090ES data link]. *Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii "Nauka segodnya: problemy i puti resheniya"* [Materials of the International scientific-practical conference "Science today: problems and solutions" (Vologda, 29 March 2017)], Vologda, 2017. Pp. 22–23. (In Russian)

7. Langejan T.P., Sunil E., Ellerbroek J., Hoekstra, J.M. Effect of ADS-B Characteristics on Airborne Conflict Detection and Resolution // 6 th SESAR Innovation: Inspiring long-term research in the field of Air Traffic Management (Netherlands, 8–10 November 2016). SESAR, 2016. Pp.1–8. URL: https://www.sesarju.eu/sites/default/files/documents/sid/2016/SIDs_2016_paper_22.pdf (date of access 05.10.2018).

8. Reck C., Reuther M.S., Jasch A., Schmidt L.P. Independent surveillance broadcast ADS-B receivers with DOA estimation. *Digital Communications – Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*. 2011. Pp. 219–222.

9. Stacey D. *Aeronautical radio communication systems and networks*. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2008. 373 p.

10. Vichujagin V.B., Rubtsov D.V. The method of calculating the statistical characteristics of the ATC system data link with automatic dependent surveillance. *Science Bulletin of Moscow State Technical University of Civil Aviation (MSTUCA)*. 2006. No. 107. Pp. 165–169. (In Russian)

11. Seybold J.S. *Introduction to RF propagation.* John Wiley & Sons Inc. Hoboken, New Jersey. 2005. 330 p.

12. Simon K.M. *Mohamed-Slim A. Digital communication over fading channels: a unified approach to performance analysis*. John Wiley & Sons Inc. Hoboken, New Jersey. 2005. 900 p.

13. Naganawa J., Miyazaki H., Tajima H. Measurement-Based Evaluation on Detection Probability of Extended Squitter for Air-to-Ground Surveillance. *Vehicular Technology IEEE Transactions*. 2017. Vol. 66. No. 10. Pp. 8883–8894.

14. Zatuchni D.A., Logvin A.I. Definition of optimum number of lines for broadcasting data for realization of ads regim. *Naučnyj vestnik MGTU GA* [Civil Aviation High TECHNOLOGIES]. 2013. No. 189. Pp. 9–13. (In Russian)

15. Zatuchni D.A. Povyshenie tochnosti otsenki dostovernosti informatsii, peredavaemoy pri avtomaticheskom zavisimom nablyudenii, na osnove analiza kachestva dopolnitel'nykh dannykh [Improving the accuracy of reliability assessment of information transmitted by automatic dependent surveillance, based on the analysis of the quality of additional data]. *Nadejnost i katchestvo slojnih system* [Reliability & Quality of Complex Systems]. 2017. No. 1. Pp. 1–16. (In Russian)

16. Netchaev E.E., Budikin U.A. *Antennie ustroistva v grajdanskoi aviacii* [Antenna systems in civil aviation]. Kursk: Press-fact. 2005. 380 p. (In Russian).

17. Zhang Z. Optimization performance analysis of 1090ES ADS-B signal separation algorithm based on PCA and ICA. *International Journal of Performability Engineering*. 2018. Vol. 14. No. 4. Pp. 741–750.

18. Kuzmin B.I. *Aviacionnaya cifrovaya elektrosvyaz v usloviah realizacii "Koncepcii ICAO-IATA CNS/ATM" v Rossiiskoi Federacii* [Aviation digital telecommunication in the conditions of implementation of the "ICAO-IATA CNS/ATM Concept" in the Russian Federation]. St. Peterburg, N. Novgorod: Vit-print. 2007. 384 p. (In Russian).

19. Schafer M., Lenders V., and Martinovic I. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. *Applied Cryptography and Network Security*. Springer. 2013. Pp. 253–271.

20. McCallie D., Butts J., Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*. 2011. Vol. 4. No. 2. Pp. 78–87.

21. Leonardi M., Piracci E., Galati G. ADS-B vulnerability to low cost jammers: risk assessment and possible solutions. *Tyrrhenian International Workshop on Digital Communications – Enhanced Surveillance of Aircraft and Vehicles*. IEEE, 2014. Pp. 41–46.

15. Zatuchni D.A. Povyshenie tochnosti otsenki dostovernosti informatsii, peredavaemoy pri avtomaticheskom zavisimom nablyudenii, na osnove analiza kachestva dopolnitel'nykh dannykh [Improving the accuracy of reliability assessment of information transmitted by automatic dependent surveillance, based on the analysis of the quality of additional data]. *Nadejnost i katchestvo slojnih system* [Reliability & Quality of Complex Systems]. 2017. No. 1. Pp. 1–16. (In Russian)

16. Netchaev E.E., Budikin U.A. *Antennie ustroistva v grajdanskoi aviacii* [Antenna systems in civil aviation]. Kursk: Press-fact. 2005. 380 p. (In Russian)

17. Zhang Z. Optimization performance analysis of 1090ES ADS-B signal separation algorithm based on PCA and ICA. *International Journal of Performability Engineering*. 2018. Vol. 14. No. 4. Pp. 741–750.

18. Kuzmin B.I. *Aviacionnaya cifrovaya elektrosvyaz v usloviah realizacii "Koncepcii ICAO-IATA CNS/ATM" v Rossiiskoi Federacii* [Aviation digital telecommunication in the conditions of implementation of the "ICAO-IATA CNS/ATM Concept" in the Russian Federation]. St. Peterburg, N. Novgorod: Vit-print. 2007. 384 p. (In Russian)
19. Schafer M., Lenders V., and Martinovic I. Experimental Analysis of Attacks on Next Generation Air Traffic Communication. *Applied Cryptography and Network Security*. Springer. 2013. Pp. 253–271.
20. McCallie D., Butts J., Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*. 2011. Vol. 4. No. 2. Pp. 78–87.
21. Leonardi M., Piracci E., Galati G. ADS-B vulnerability to low cost jammers: risk assessment and possible solutions. *Tyrrhenian International Workshop on Digital Communications – Enhanced Surveillance of Aircraft and Vehicles*. IEEE. 2014. Pp. 41–46.

INFORMATION ABOUT AUTHORS:
Rubtsov E.A., PhD, Associate Professor at the Department of Radio electronic systems, St. Petersburg State University of civil aviation;
Kalintsev A.S., Applicant at the Department of Radio electronic systems, St. Petersburg State University of civil aviation;
Grigorevs E.I., Senior lecturer of the Department of Radio electronic systems, St. Petersburg State University of civil aviation.

For citation: Rubtsov E.A., Kalintsev A.S., Grigorevs E.I. Data link analysis of automatic dependent surveillance – broadcast. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 19–27. doi: 10.24411/2409-5419-2018-10184 (In Russian)

doi: 10.24411/2409-5419-2018-10185

Организация процедур по выявлению и локализации нарушений политик безопасности при управлении безопасностью функционирования подсистемы обеспечения единым временем автоматизированной системы управления сложной организационно-технической системой

БУРЕНИН
Андрей Николаевич[1]

ЛЕГКОВ
Константин Евгеньевич[2]

ПЕРВОВ
Михаил Сергеевич[3]

АННОТАЦИЯ

Наблюдающееся в настоящее время регулярные попытки различных нарушителей повлиять на нормальное функционирование корпоративных и ведомственных сложных организационно-технических систем с помощью разного рода информационных воздействий (системных, сетевых и компьютерных атак), вызывают необходимость применения комплекса мер и программно-аппаратных комплексов, обеспечивающих их безопасность. При этом наиболее подвержены атакам самые критически важные элементы сложных организационно-технических систем, к числу которых относится автоматизированная система управления системой и ее подсистемы. Среди всех подсистем особо выделяется подсистема обеспечения единым временем, нарушение работы которой разного рода атаками может привести к срыву управления всей организационно-технической системой и дезорганизации ее функционирования. Требуемый уровень противодействий атакам на подсистему обеспечения единым временем автоматизированной системы управления может быть обеспечен не только созданием эффективной системы комплексной безопасности, но и созданием специальных комплексов управления безопасностью, одними из наиболее важных функций которых являются функции управления политиками безопасности. В работе рассматриваются основные задачи управления политиками безопасности в части оперативного поиска нарушений, которые необходимо решить при организации качественной работы подсистемы обеспечения единым временем активных элементов автоматизированной системы управления, участвующих в процессах управления современной организационно-технической системой специального назначения, в условиях воздействия на подсистему обеспечения единым временем атак высокой интенсивности.

КЛЮЧЕВЫЕ СЛОВА: кибератака; . вероятностно-временны характеристики; автоматизированная система управления; система защиты; программные воздействия.

Сведения об авторах:

[1]д.т.н., профессор, главный специалист Акционерного общества «Научно-исследовательский институт «Рубин», г. Санкт-Петербург, Россия, konferencia_asu_vka@mail.ru

[2]к.т.н., доцент, начальник кафедры автоматиздтрованных систем управления Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, constl@mail.ru

[3]Военная академия связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия

Для цитирования: *Буренин А.Н., Легков К.Е., Первов М.С.* Организация процедур по выявлению и локализации нарушений политик безопасности при управлении безопасностью функционирования подсистемы обеспечения единым временем автоматизированной системы управления сложной организационно-технической системой // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 28–36. doi: 10.24411/2409-5419-2018-10185

Введение

В современных условиях резко возрастает вероятность существенного изменения характера функционирования корпоративных и ведомственных сложных организационно-технических систем специального назначения, под воздействием высокоинтенсивных атак на автоматизированные системы управления (АСУ) ими в целом или на наиболее критически важные подсистемы АСУ. Среди таких подсистем особо выделяется подсистема обеспечения единым временем (ПО ЕВ) [1–3], нарушение работы которой разного рода атаками может привести к срыву управления корпоративной или ведомственной сложной организационно-технической системой (СОТС).

Требуемое противодействие атакам на ПО ЕВ АСУ СОТС не может быть обеспечено только созданием эффективной системы комплексной безопасности. Необходимо также создать еще специальную подсистему управления безопасностью, одной из наиболее важных функций которой является функция управления политиками безопасности [4, 5–20]. При этом под политикой (совокупность частных политик) безопасности ПО ЕВ в работе понимается основной документ, в котором описаны все правила безопасности и который разрабатывается, утверждается, хранится в течение определенного срока, отражается в соответствующей базе данных системы управления и, который обеспечивает нормальное функционирование подсистемы единого времени в условиях прогнозируемых атак нарушителей, если их номенклатура и интенсивность не выходят за рамки, предусмотренных политикой.

При управлении политиками безопасности в ПО ЕВ особо важным является выявление нарушений действующей в ПО ЕВ АСУ СОТС политики, которые происходят по многочисленным причинам, учесть которые практически невозможно. В силу этого необходимы независимые механизмы оперативного выявления и локализации этих нарушений, что, несомненно, скажется положительно на качестве управления безопасностью и на уровне безопасности ПО ЕВ в целом.

Место и роль задачи поиска и локализации нарушений политик безопасности

Подсистема обеспечения единым временем, как правило, носит распределенный по компонентам АСУ СОТС характер. Поэтому и система обеспечения комплексной безопасности ПО ЕВ будет содержать несколько серверов управления безопасностью, а само управление политиками будет также распределенным и должно выполнять принятую в ПО ЕВ политику безопасности, представляющую собой совокупность частных политик безопасности (ЧПБ) во всех компонентах подсистемы, осуществляя регулярный контроль выполнения ЧПБ, постоянный мониторинг событий безопасности (признанных инцидентами) и принимая решение о будущей корректировке ЧПБ.

Подзадача управления безопасностью ПО ЕВ в рамках уже действующей политики безопасности, как совокупности ЧПБ для каждого ее компонента, можно определить как реализацию набора определенных правил, сформулированных для всех объектов защиты.

Обычно проведение текущего аудита безопасности ПО ЕВ, обеспечивающего получение и оценку объективных данных о текущем состоянии защищенности подсистемы и соблюдении действующей политики безопасности, осуществляется по плану и достаточно редко, поэтому актуальной становится задача оперативного контроля выполнения политик безопасности в процессе функционирования подсистемы с высокой степенью автоматизации процессов поиска и локализации нарушений.

Организация управления поисками локализацией нарушений политик безопасности

Ясно, что среди задач управления политиками безопасности в ПО ЕВ АСУ СОТС в рамках действующей политики, одной из наиболее важных является задача управления, в основу которой положены модели и методы локализации возможных нарушений в программных и технических средствах ПО ЕВ, которые позволяют осуществлять поиск и локализацию, появляющихся во время ее эксплуатации различных нарушений ЧПБ.

Вместе с тем, достаточно большое количество компонентов и элементов ПО ЕВ и связей между ними, охваченных комплексами обеспечения и контроля безопасности, исключает возможность «подетальной» проверки выполнение требований всех ЧПБ во время эксплуатации подсистемы. Однако, ограниченная надежность программно-аппаратных средств обеспечения безопасности и подверженность их различным воздействиям нарушителей, приводит к необходимости проведения независимой оценки степени выполнения ЧПБ в подсистеме.

Это можно осуществить проведением периодических тестовых испытаний этих средств для исключения случаев, когда возможны нарушения действующей политики безопасности, несмотря на отсутствие предупреждений со стороны подсистемы обеспечения безопасности. Естественно, что целью таких тестовых испытаний является выделение с возможно большей точностью источника нарушений действующей политики безопасности, а сами задачи поиска и выделения источника нарушения (элемента, фрагмента, комплекса) целесообразно решать специально развернутыми комплексами средств диагностики в составе подсистемы управления безопасностью ПО ЕВ АСУ СОТС. При этом оператор АРМ управления безопасностью ПО ЕВ или ДЛ по безопасности органа управления СОТС во время поиска нарушившего требования политики безопасности элемента, фрагмента или комплекса с помощью соответствующих средств автоматизации производит

тестовые испытания и сравнивает результаты испытаний с требованиями той или иной ЧПБ. Затем осуществляется анализ и сопоставление результатов испытаний и по ним определяется объект, ставший причиной нарушения требований данной ЧПБ. Этими процедурами осуществляется локализация последствий не преднамеренных или преднамеренных действий, приведших к нарушению действующих ЧПБ. Поэтому обязательным элементом управления безопасностью ПО ЕВ АСУ СОТС, в рамках действующих ЧПБ, являются процедуры диагностики нарушений безопасности, которые реализуют рациональные методы распознания не безопасного состояния.

К основным задачам диагностики нарушений ЧПБ относятся:

– определение наиболее информативных испытаний объектов и субъектов безопасности ПО ЕВ;

– определение рациональной последовательности контроля;

– поиск элемента, компонента или комплекса, ставших причиной нарушения ЧПБ;

– выбор и расстановка схем программно-аппаратных комплексов контроля;

– рациональное разделение ПО ЕВ АСУ СОТС на контролируемые зоны;

– максимальная автоматизация процессов контроля.

В случае отрицательного результата испытания любого объекта, можно только сделать вывод, что появились некоторый симптом нарушения частной политики безопасности и в первом приближении место этого нарушения, т. к. источник (или причина) нарушения может находиться либо в контролируемом объекте, либо в одном из предшествующих ему объектов (элементов, фрагментов, компонентов), а это означает, что нарушение не может быть исправлено в последующих после источника объектах и тем или иным образом вызывает невыполнение требований безопасности во всей рассматриваемой цепи ПО ЕВ АСУ СОТС. Ясно, чем меньше трудоемкость испытаний, тем меньше общие затраты ресурсов системы управления на контроль и поиск нарушений безопасности того или иного элемента, фрагмента или компонента ПО ЕВ АСУ СОТС. Поэтому наиболее критичные объекты ПО ЕВ АСУ СОТС целесообразно оснастить подчиненных центру управления политиками специальными программно-аппаратными модулями контроля, являющимися элементами подсистемы управления безопасностью. Встроенные модули обеспечивают полную или частичную оценку функционирования контролируемого критичного объекта ПО ЕВ АСУ СОТС в плане выполнения им приписанных ему требований безопасности. Показания встроенных модулей являются активными признаками выполнения или невыполнения требований.

Однако, как правило, в реальных АСУ СОТС число таких модулей обычно недостаточно для полного контроля ПО ЕВ. Поэтому наряду с активными признаками целесообразно использовать определенные контрольные точки и пассивные признаки, по которым можно косвенно судить о соблюдения требований безопасности.

Различные элементы, фрагменты, компоненты ПО ЕВ АСУ СОТС имеют специфические особенности в плоскости реализации ЧПБ, что отражается в особенностях пассивных признаков. Однако отсутствие практической возможности количественной оценки множества пассивных признаков выполнения или не выполнения требований ЧПБ не лишает их достаточной объективности и возможности простой бинарной оценки (да — нет) выявления нарушений.

В целом любые процедуры по локализации объектов нарушения действующей в ПО ЕВ АСУ СОТС политики безопасности целесообразно разделить на ряд операций детерминированных (имеющих только один возможный результат) и альтернативных (предполагающих принятие решения о дальнейших действиях). Причем процедуры по поиску объекта «нарушителя» действующих ЧПБ в основном состоят из избирательных операций — испытаний в различных фрагментах ПО ЕВ АСУ СОТС.

Модели испытаний по контролю исполнения ЧПБ в ПО ЕВ АСУ СОТС

Испытания по контролю исполнения ЧПБ в ПО ЕВ АСУ СОТС должны осуществляться в определенной последовательности поиска, которая завершается выделением элемента с нарушением ЧПБ. Особенностью последовательности поиска для ПО ЕВ АСУ СОТС является существенное разветвление ее в каждом испытании. Поэтому совокупность всех разветвлений образует ветвящуюся структуру, так называемое дерево возможностей поиска нарушений ЧПБ в ПО ЕВ АСУ СОТС, число различных ветвей которого равно числу различных возможных нарушений и изменений в контролируемых зонах безопасности.

В общем случае от начала испытаний к каждому нарушению безопасности ведут различные по содержанию последовательности поиска. При этом каждая последовательность поиска имеет два количественных параметра (рис. 1):

– число испытаний в последовательности k_i;

– суммарная длительность последовательности испытаний $T_i = \sum_{k=1}^{k_i} t_k$, а t_k — длительность i-го тестового испытания.

В целом суммарные длительности последовательностей оказываются не равными друг другу, а число испытаний в последовательностях поиска зависит от формы дерева логических возможностей поиска нарушений политик безопасности в ПО ЕВ АСУ СОТС и также могут ока-

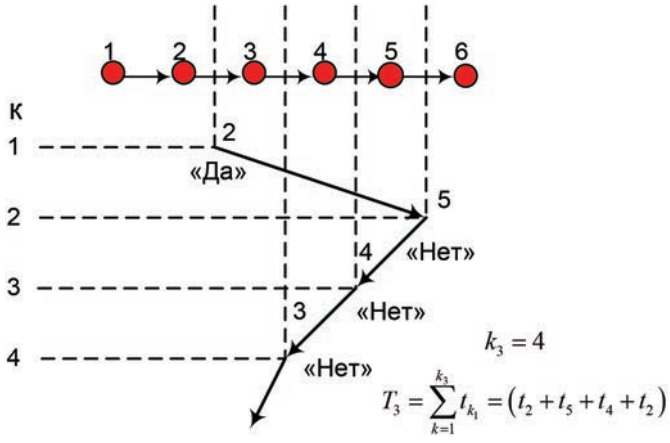


Рис. 1. Последовательность поиска нарушений политик безопасности

заться не равными друг другу. Поэтому дерево логических возможностей поиска нарушений политик безопасности в ПО ЕВ АСУ СОТС целесообразно оценить двумя показателями: средним числом испытаний в последовательности поиска любого нарушения и средней длительностью последовательности поиска.

Вероятности нарушений политик безопасности и изменений в контролируемых зонах безопасности ПО ЕВ АСУ СОТС в общем случае отличаются друг от друга. Поэтому в качестве значений параметров можно применить математические ожидания длины и длительности последовательности поиска. При этом целесообразно исходить из следующих соображений: если *i*-й объект является источником нарушения политики безопасности в комплексе ПО ЕВ АСУ СОТС с вероятностью $p(H_{i/x})$, то с этой же вероятностью реализуется *i*-я последовательность поиска, приводящая к этому объекту. Следовательно, если известны все длины и длительности последовательностей поиска и их вероятности, то математическое ожидание длины последовательности поиска нарушений составит:

$$m_k = \sum_{i=1}^{L} p\left(H_{i/x}\right) k_i. \qquad (2)$$

А математическое ожидание длительности поиска будет равно

$$m_T = L_{\text{ПОЕТ}}^{NPb} \sum_{i=1}^{L} p\left(H_{i/x}\right) T_i = \sum_{i=1}^{L_{\text{ПОЕТ}}^{NPb}} p\left(H_{i/x}\right) \sum_{k=1}^{k_i} t_k, \qquad (3)$$

где $L_{\text{ПОЕТ}}^{NPb}$ — число различных возможных нарушений политик безопасности в ПО ЕВ АСУ СОТС.

В частном случае, если вероятности $p(H_{i/x})$ равны для всех нарушений политик безопасности (или неизвестны), то математические ожидания оценивают средними значениями:

$$p\left(H_{i/x}\right) = p\left(H_x\right) = \frac{1}{L_{\text{ПОЕТ}}^{NPb}}, \qquad (4)$$

$$m_k = \sum_{i=1}^{L_{\text{ПОЕТ}}^{NPb}} \frac{1}{L_{\text{ПОЕТ}}^{NPb}} k_i = \frac{1}{L_{\text{ПОЕТ}}^{NPb}} \sum_{i=1}^{L_{\text{ПОЕТ}}^{NPb}} k_i, \qquad (5)$$

$$m_T = \sum_{i=1}^{L_{\text{ПОЕТ}}^{NPb}} \frac{1}{L_{\text{ПОЕТ}}^{NPb}} T_i = \frac{1}{L_{\text{ПОЕТ}}^{NPb}} \sum_{i=1}^{L_{\text{ПОЕТ}}^{NPb}} T_i. \qquad (6)$$

Длины последовательностей поиска определяют глубину поиска, а число различных нарушений политик безопасности под воздействием различных факторов в объекте ПО ЕВ АСУ СОТС $L_{\text{ПОЕТ}}^{NPb}$, как правило, отличается от числа элементов, компонентов, комплексов ПО ЕВ АСУ СОТС, т.к. в одном и том же объекте ПО ЕВ может быть нарушение разных требований политик безопасности, фиксация каждого из которых различаются по способам поиска, если даже территориально они появляются в одном компоненте. Таким образом, число нарушений ЧПБ и изменений в контролируемых кластерах безопасности, а также число последовательностей поиска отличаются от числа элементов в объектах ПО ЕВ АСУ СОТС, по крайней мере, в несколько раз.

Так как объекты ЧПБ в ПО ЕВ АСУ СОТС связаны друг с другом, то, как правило, возникновение нарушений в одном из них проявляется в искажении или нарушении ЧПБ в ряде других объектов, что можно использовать при организации поиска. Поэтому целесообразно представлять, что нарушения ЧПБ образуют структурную модель в виде ориентированного графа. При этом часть модели, непосредственно связанная с изменениями в контролируемых компонентах ПО ЕВ АСУ СОТС, представляет собой структурно-функциональную модель, в которой объекты считаются источниками нарушений и связаны между собой естественными последовательностями. Другая часть модели нарушений представляет собой совокупность объектов ПО ЕВ АСУ СОТС, которые являются причинами нарушений в других объектах и связаны между собой в направлении, противоположном естественному распространению информации при поиске.

Модель взаимосвязи объектов нарушений ЧПБ целесообразно задать пространством поиска. Представление этого пространства в форме ориентированного графа дает возможность точно определить координату каждого источника нарушений и связь его с другими возможными источниками и объектами. В этом случае пространством поиска в задачах локализации нарушений ЧПБ является вся ПО ЕВ АСУ СОТС, не смотря на то, что преднамерен-

ное нарушение, вызванное атаками нарушителей, направлено на определенный сегмент или компонент подсистемы или систему управления ПО ЕВ. Тогда пространство всей подсистемы может быть представлено в форме ориентированного графа $G_{P\sec}(E_{P\sec}, T_{P\sec})$, который определяет связи между объектами безопасности ПО ЕВ АСУ СОТС (вершины $E_{P\sec}$) и показывает взаимозависимость между признаками работы в соответствии с действующими ЧПБ и симптомами их нарушения.

При проведении тестовых испытаний на выявление нарушений ЧПБ целесообразно пространство разделить на две независимые части. Затем последовательное деление пространства поиска за конечное число шагов приводит к элементарному участку пространства поиска, который и является объектом — источником нарушения ЧПБ. Отсюда следует, что дерево логических возможностей поиска нарушений ЧПБ в ПО ЕВ АСУ СОТС, формирующееся при поиске нарушений, возникающих под воздействием различных факторов, имеет прямую связь с пространством поиска.

Типичное для ПО ЕВ большинства АСУ СОТС число базовых нарушений ЧПБ составляет $L_{\text{ПОЕТ}}^{NPb} \approx 6-10$. При этом пространство поиска содержит 6 элементов с одним входным и одним выходным элементами.

Дерево логических возможностей поиска нарушений ЧПБ в ПО ЕВ АСУ СОТС представляет собой ветвящуюся геометрическую структуру с одной входной вершиной и $L_{\text{ПОЕТ}}^{NPb}$ выходными вершинами. Представление процедур поиска в виде деревьев позволяет на основании логических умозаключений прийти к одному из нескольких возможных решений, т.к. в принципе, любой процесс принятия решения при управлении безопасностью ПО ЕВ АСУ СОТС можно представить в виде дерева логических возможностей. При поиске элемента, компонента, комплекса, в которых произошло нарушение ЧПБ, необходимо принять решение об устранении этого (этих) нарушения или даже замене оборудования, поэтому процесс тестовых испытаний ПО ЕВ АСУ СОТС и логический анализ их результатов входят в диагностику нарушений ЧПБ как главная составная часть.

Для дерева логических возможностей поиска нарушений ЧПБ в ПО ЕВ АСУ СОТС можно привести математическую связь между параметрами, выражаемую формулой:

$$L_{\text{ПОЕТ}}^{NPb}(m,n) = (m-1)\,n+1, \tag{7}$$

где $L_{\text{ПОЕТ}}^{NPb}(m,n)$ — число различных ветвей в дереве;
n — число единичных выборов;
m — модули единичных выборов.

Перед началом тестовых испытаний при поиске нарушений требований всех ЧПБ ПО ЕВ существует неопределенность относительно того, в какой части ее находится объект с нарушением. Если вероятности нарушения ЧПБ для объектов одинаковы, то эта неопределенность (или энтропия) равна

$$H(k, L_{\text{ПОЕТ}}^{NPb}) = \log_2 L_{\text{ПОЕТ}}^{NPb}. \tag{8}$$

После проведения в среднем k тестовых испытаний энтропия становится равной нулю, так как к этому моменту объект с нарушением требований ЧПБ уже будет локализирован и неопределенность относительно положения этого объекта будет устранена.

Если вероятности различных результатов поиска нарушений ЧПБ $p(H_{l/x})$ оказываются неравными друг другу, то энтропия перед началом поиска равна:

$$H(k, L_{\text{ПОЕТ}}^{NPb}) = -\sum_{i=1}^{L} p(H_{l|x}) \log_2 p(H_{l|x}). \tag{9}$$

Необходимо обеспечить минимум среднего значения длины последовательности поиска при неравных вероятностях $p(H_{l/x})$. Для этого необходимо, чтобы выполнялось приближенное равенство: $k_i \approx -\log_2 p(H_{l|x}), \forall\, i = 1, 2, ..., L,$ а это означает, что длина оптимизированных по вероятностям последовательностей поиска фактов нарушений ЧПБ в ПО ЕВ АСУ СОТС связана обратной зависимостью с вероятностями появлений нарушений ЧПБ в объектах подсистемы, к которым они ведут.

В целом при построении процедур поиска фактов нарушений ЧПБ в ПО ЕВ АСУ СОТС важным является построение формальных планов и программ поиска объекта (объектов) с нарушением ЧПБ. Естественно выбирают такой план, который минимизирует среднюю длину последовательности поиска.

В случае преднамеренных скрытых нарушений, осуществленных внутренним нарушителем, при непосредственном контроле фактов нарушений ЧПБ, в числе применяемых на практике методов тестовых испытаний, с целью выявления объектов ПО ЕВ АСУ СОТС с нарушением требований ЧПБ, можно применять метод пробных подмен объектов объектами со стандартным (в соответствии с действующей ЧПБ) набором правил безопасности.

Однако, тестовое испытание, состоящее в пробной замене, всегда отделяет от контролируемого компонента только один объект, и могут возникнуть трудности по дистанционному подключению эталонного объекта, особенно если этот объект заменяет достаточно сложный фрагмент (компонент) ПО ЕВ АСУ СОТС. В этом случае целесообразно использовать заранее созданные программно-аппаратные имитаторы объектов.

Если в ПО ЕВ АСУ СОТС имеет место группа фактов нарушений ЧПБ (как правило, более 3–4), привязанных к соответствующим объектам, то:

$$M_{Q_{\text{ПОЕТ}}^{Pb}} = \{j_1, j_2, ..., j_Q\} \in M_{\text{ПОЕТ}}^{Pb}, \qquad (10)$$

где $M_{\text{ПОЕТ}}^{Pb}$ — множество объектов с ЧПБ, а индексы j_q в $M_{Q_{\text{ПОЕТ}}^{Pb}}$ соответствуют объектам с нарушением ЧПБ следующим образом: j обозначает порядковый номер объекта (компонента) в ПО ЕВ АСУ СОТС, а q — номер объекта с нарушением ЧПБ, величина которого меняется в пределах от 1 до $Q_{\text{ПОЕТ}}^{Pb}$ и возрастает от первого объекта с нарушением ЧПБ к последнему объекту.

При этом, сколько бы ни было других объектов с нарушением ЧПБ, процедура поиска объекта с индексом j_1 строится так же, как процедура поиска одного объекта. После завершения поиска и восстановления требований ЧПБ в объекте с индексом j_1 множество $M_{\text{ПОЕТ}}^{Pb}$ сократится на один объект, при этом множество элементов в пространстве поиска также сократится и поиск следующего объекта с нарушением ЧПБ, имеющего индекс $j_2 j_2$, происходит уже не во всей подсистеме единого времени АСУ СОТС, а только в той части, которая следует за восстановленным объектом j_1. При этом процедура поиска оптимизируется на множестве М1, имеющем $L_{\text{ПОЕТ}}^{NPb} - j_1$ объектов, из которых только в $Q_{\text{ПОЕТ}}^{Pb} - 1$ присутствуют нарушения ЧПБ.

В дальнейшем процедуры поиска и восстановления выполнения требований ЧПБ в объектах с их нарушениями продолжаются до того момента, когда будет выделен и восстановлен последний объект, имеющий индекс j_q.

Так как число одновременно имеющихся в ПО ЕВ АСУ СОТС нарушений ЧПБ случайно и заранее неизвестно, то после восстановления требований в каждом объекте целесообразно проводить проверку многих параметров безопасности, записанных в ЧПБ. Отсюда следует, что число различных исходов (результатов) поиска при неординарном случайном потоке нарушений ЧПБ зависит от $Q_{\text{ПОЕТ}}^{Pb} > 1$ и $L_{\text{ПОЕТ}}^{NPb}$, а так как при проводимых поисковых испытаниях применяются бинарные оценки, то очевидно, что число исходов поиска является суммой биномиальных коэффициентов

$$K(L_{\text{ПОЕТ}}^{NPb}, Q) = \sum_{l=1}^{Q} C_{L_{MCCCH}^{NPb}}^{l}. \qquad (11)$$

Таким образом, оптимизацию процедур поиска нескольких объектов ПО ЕВ АСУ СОТС с нарушениями ЧПБ целесообразно происходить раздельно при осуществлении поиска каждого объекта. При этом пространство поиска, после обнаружения объекта и восстановления требований ЧПБ в нем, сокращается, а суммарная длина ветвей процедуры поиска $Q_{\text{ПОЕТ}}^{Pb}$ объектов ПО ЕВ АСУ СОТС с нарушением ЧПБ составит:

$$K_{\Sigma}(L_{\text{ПОЕТ}}^{NPb}, Q_{\text{ПОЕТ}}^{Pb}) = \sum_{l=1}^{Q} C_{L_{MCCCH}^{NPb}}^{l} + ... + \\ + \sum_{j_1}^{L_{MCCCH}^{NPb}} ... \sum_{j_q}^{L_{MCCCH}^{NPb}} K_{\Sigma}(L_{\text{ПОЕТ}}^{NPb} - j_q, Q_{\text{ПОЕТ}}^{Pb} - q). \qquad (12)$$

Рассмотренные процедуры поиска элементов ПО ЕВ АСУ СОТС с нарушениями ЧПБ в различных ее компонентах, позволяют в значительной степени автоматизировать процессы управления безопасностью ПО ЕВ АСУ СОТС в части управления политиками и тем самым увеличить оперативность и своевременность выявления нарушений, а также повысить устойчивость функционирования подсистемы в плане безопасности (путем оперативного снижения числа потенциально успешных атак нарушителей, вызванных уязвимостями из-за невыполнения требований ЧПБ), рис. 2.

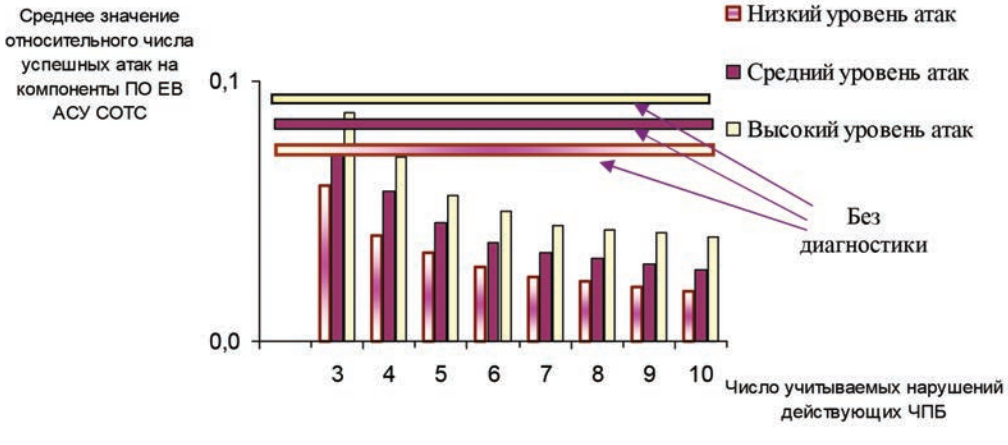


Рис. 2. Эффективность проведения процедур централизованной диагностики нарушений действующей политики безопасности ПО ЕВ АСУ СОТС в разное время

Выводы

Обеспечение безопасности функционирования подсистемы АСУ СОТС, гарантирующей предоставления требуемых метрик времени, предполагает осуществление процедур управления частными политиками безопасности (ЧПБ).

При управлении политиками безопасности в ПО ЕВ АСУ СОТС особо важным является выявление нарушений действующей политики, которые происходят по многочисленным причинам, учесть которые практически невозможно. В силу этого необходимы механизмы оперативного выявления и локализации этих нарушений, что, несомненно, скажется положительно на качестве управления безопасностью и на уровне безопасности ПО ЕВ.

Модель взаимосвязи объектов нарушений ЧПБ задается пространством поиска, а представление этого пространства в форме ориентированного графа дает возможность точно определить координату каждого источника нарушений и связь его с другими возможными источниками и объектами. В этом случае пространством поиска в задачах локализации нарушений ЧПБ является вся ПО ЕВ АСУ СОТС, не смотря на то, что преднамеренное нарушение, вызванное атаками нарушителей, направлено на определенный сегмент или компонент подсистемы или систему управления ею.

Объекты ПО ЕВ АСУ СОТС связаны друг с другом, и, как правило, возникновение нарушений ЧПБ в одном из них проявляется в искажении или нарушении ЧПБ в ряде других объектов. Этот факт можно использовать при организации поиска.

При построении процедур поиска фактов нарушений ЧПБ в ПО ЕВ АСУ СОТС построение формальных планов или программ поиска объекта с нарушением ЧПБ осуществляют из условия минимизации средней длины последовательности поиска.

После окончания процессов локализации фактов нарушений ЧПБ, решение задач восстановления безопасной работоспособности ПО ЕВ АСУ СОТС представляется в виде многоэтапной процедуры, включающей подключение ресурсов взамен скомпрометированных, обращение к подсистеме управления структурой подсистемы, корректировку исходных данных, восстановление требований ЧПБ в объекте с нарушением и пр.

Литература

1. Система Единого времени для спецпотребителей. URL: www: chas.prom.com (дата обращения 01.10.2018).

2. Система единого времени «Интелтек Плюс». URL: http://www.inteltec.ru/. (дата обращения 01.10.2018).

3. *Буренин А.Н., Голубев В.Е., Легков К.Е.* Организация подсистемы обеспечения единым временем решающих элементов автоматизированной системы управления сложными организационно-техническими объектами специального назначения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 2. С. 27–34.

4. *Буренин А.Н., Легков К.Е.* Современные инфокоммуникационные системы и сети специального назначения. Основы построения и управления. М.: Медиа Паблишер, 2015. 348 с.

5. *Буренин А.Н., Курносов В.И.* Теоретические основы управления современными телекоммуникационными сетями. М.: Наука. 2011. 464 с.

6. *Ушаков И.А.* Вероятностные модели надежности информационно-вычислительных систем. М.: Радио и связь, 1991. 132 с.

7. *Феллер В.* Введение в теорию вероятностей и ее приложения. М.: Мир. 1984. 1 т. 528 р

8. *Шнепс-Шнеппе М.А.* Системы распределения информации. Методы расчета. М.: Связь. 1979. 342 с.

9. *Емельянов А.В., Легков К.Е., Оркин В.В.* Анализ проблем информационной безопасности информационных систем специального назначения при управлении ими // Труды II Межвузовской научно-практической конференции «Проблемы технического обеспечения войск в современных условиях». СПб.: Военная академия связи, 2017. С. 122–126.

10. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. 592 с.

11. *Ерохин С.Д., Артамонова Я.С., Легков К.Е.* К вопросу о методике выявления угроз информационной безопасности в пограничном пространстве // I-methods. 2013. Т. 5. № 2. С. 19–22.

12. *Бабошин В.А., Сиротенко Ф.Ф.* Модель процесса мониторинга транспортной сети специального назначения на основе нечеткой логики // I-methods. 2013. Т. 5. № 1. С. 20–25.

13. *Ерохин С.Д., Легков К.Е.* Информационные угрозы автоматизированных систем управления технологическими процессами // I-methods. 2014. Т. 6. № 1. С. 24–26.

14. *Корсунский А.С., Масленникова Т.Н., Ерышов В.Г.* Модель системы анализа защищенности информации в автоматизированных системах // I-methods. 2015. Т. 7. № 4. С. 30–34.

15. *Mitra D., Ramakrishman K.G.* Technics for traffic engeniring of multiservice in priority networks // BLTJ. 2001. Vol. 1. Pp. 123–130.

16. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Безопасность глобальных сетевых технологий. СПб.: СПбУ, 1999. 234 с.

17. *Котенко И.В., Степашкин М.В., Богданов В.С.* Анализ защищенности компьютерных сетей на раз личных этапах проектирования и эксплуатации // Изв. вузов. Приборостроение. 2006. Т. 49. № 5. С. 3–8.

18. *Gorodetsky V., Kotenko I., Karsayev O.* The Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning // The International Journal of Computer Systems Science &Engineering. 2003. Vol. 18. № 4. Pp. 191–200.

19. *Harmer P., Williams P., Gunsch G., Lamont G.B.* An artificial immune system architecture for computer security applications // IEEE Transactions on Evolutionary Computation. 2002. Vol. 6. No. 3. Pp. 252–280.

20. *Al-Kasassbeh M., Adda M.* Network fault detection with Wiener filter-based agent // Journal of Network and Computer Applications. 2009. Vol. 32. No. 4. Pp. 824–833.

The organization of procedures for identification and localization of violations of security policies at security management of functioning of a subsystem of providing with uniform time of the automated control system for a complex organizational and technical system

ANDREY N. BURENIN,
St. Petersburg, Russia, konferencia_asu_vka@mail.ru

KONSTANTIN E. LEGKOV,
St-Petersburg, Russia, constl@mail.ru

MIKHAIL S. PERVOV,
St. Petersburg, Russia

KEYWORDS: cyber attack; probable time response characteristics; automated control system; protection system; program impacts.

ABSTRACT

Regular attempts of different violators to influence the normal functioning of enterprise and departmental complex organizational and technical systems by means of any information influences (the system, network and computer attacks) which is observed now, cause the necessity of application of a package of measures and the hardware-software complexes ensuring their safety. At the same time the most crucial elements of complex organizational and technical systems which the automated control system for a system and its subsystems is among are most subject to the attacks. Among all subsystems the subsystem of providing with uniform time which violation of any work as the attacks can lead to failure of management of all organizational and technical system and disorganization of its functioning is especially selected. Required level of counteractions to the attacks on a subsystem of providing the automated control system with uniform time can be provided not only with creation of an effective system of complex safety, but also creation of special complexes of security management, one of the most important functions of which are functions of management of politicians of safety. In work the main objectives of management of security policies regarding quick search of violations which need to be solved at the organization of high-quality work of a subsystem of providing the automated control system with uniform time of the active elements participating in processes of management of the modern organizational and technical system of a special purpose in the conditions of impact on a subsystem of ensuring high intensity with uniform time of the attacks are considered.

REFERENCES

1. Sistema Edinogo vremeni dlya spechpotrebitelei [Common timing system for special consumers]. URL: www.chas.prom.com (date of access 01.10.2018). (In Russian)

2. Sistema edinogo vremeni "Inteltek Plyus" [Common timing system of Inteltek Plus]. URL: http://www.inteltec.ru/ (date of access 01.10.2018). (In Russian)

3. Burenin A.N., Golubev V.E., Legkov K.E.. The organization of the subsystem software unified time critical elements of an automated system of control of complex organizational-technical facilities for special purposes. *T-Comm*. 2018. Vol. 12. No. 2. Pp. 27–34. (In Russian)

4. Burenin A.N., Legkov K.E. *Sovremennye infokommunikatsionnye sistemy i seti spetsial nogo naznacheniya. Osnovy postroeniya I upravleniya: Monografiya* [Modern infocommunication systems and special purpose networks. Basics of creation and control]. Moscow: Media Publisher, 2015. 348 p. (In Russian)

5. Burenin A. N., Kurnosov V.I. *Teoreticheskie osnovy upravleniya sovremennymi telekommunikacionnymi setyami* [Theoretical bases of management of modern telecommunications networks]. Moscow: Nauka, 2011. 464 p. (In Russian)

6. Ushakov I.A. *Veroyatnostnye modeli nadezhnosti informatsionno-vychislitel'nykh system* [Probabilistic models of reliability of information-computing systems]. Moscow: Radio i svyaz', 1991. 132 p. (In Russian)

7. Feller W. *An Introduction to Probability Theory and its Applications*. 3rd ed. 1968. Vol. 1. 528 p.

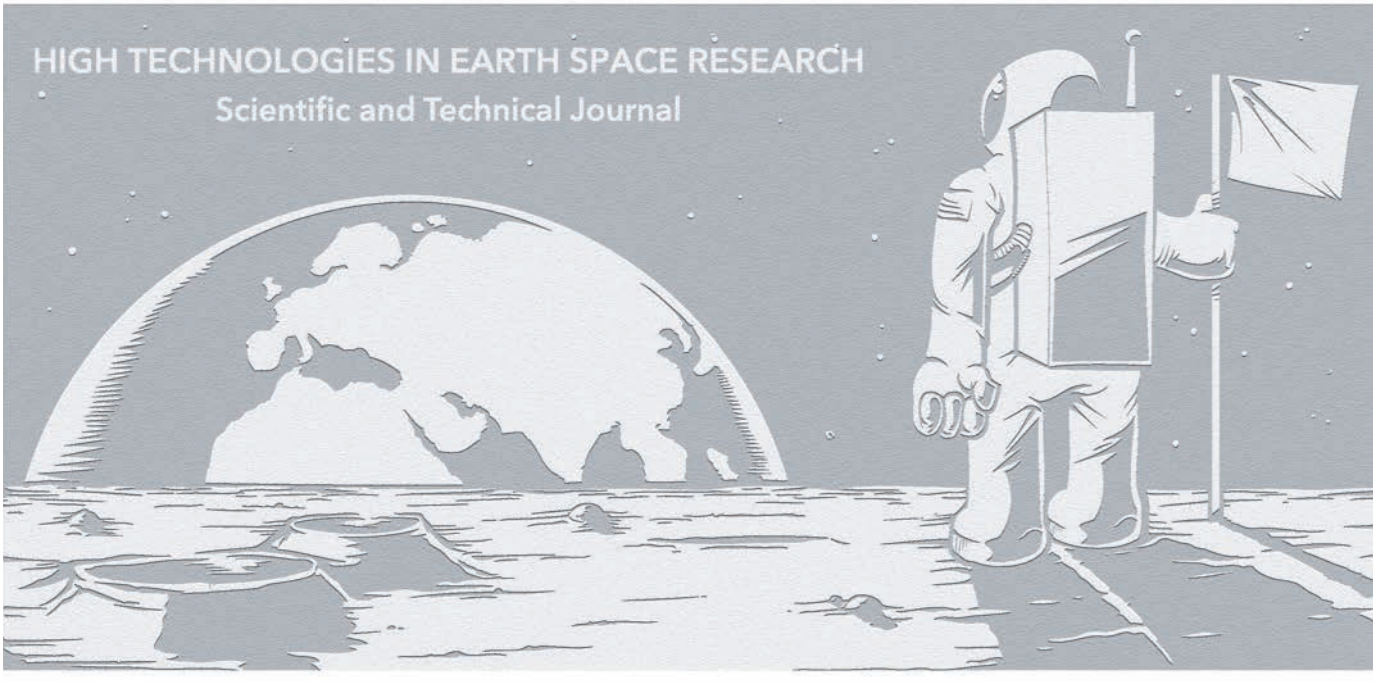
8. Shneps-Shneppe M.A. *Distribution System information. Calculation methods*. Moscow: Svyas', 1979. 342 p. (In Russian)

9. Emel'yanov A.V., Legkov K.E., Orkin V.V. Analiz problem informatsionnoy bezopasnosti informatsionnykh sistem spetsial'nogo naznacheniya pri upravlenii imi [Proceedings of the II Interuniversity scientific and practical conference «Problems of technical support of troops in modern conditions»]. *Trudy II Mezhvuzovskoy nauchno-prakticheskoy konferentsii "Problemy tekhnicheskogo obespecheniya voysk v sovremennykh usloviyakh"* [Proceedings of the II Inter-

university scientific and practical conference "Problems of technical support of troops in modern conditions"]. St. Petesburg: Voennaya akademiya svyazi, 2017. Pp. 122–126. (In Russian)
10. Shan'gin V.F. *Zashchita informatsii v komp'yuternykh sistemakh i setyakh* [Information Protection in computer systems and networks]. Moscow: DMK Press, 2012. 592 p. (In Russian)
11. Erokhin S.D., Artamonov Y.S., Legkov K.E. To the question about the methods of identification of information security threats in the border space. *I-methods*. 2013. Vol. 5. No. 2. Pp. 19–22. (In Russian)
12. Baboshin V.A., Sirotenko F.F. The model of the process of monitoring the transportation network for special purposes based on fuzzy logic. *I-methods*. 2013. Vol. 5. No. 1. Pp. 20–25. (In Russian)
13. Erokhin S.D., Legkov K.E. Information threats are automated systems of control of technological processes. *I-methods*. 2014. Vol. 6. No. 1. Pp. 24–26. (In Russian)
14. Korsun A.S., Maslennikova T.N., Erychov V.G. Model system analysis of information security in automated systems. *I-methods*. 2015. Vol. 7. No. 4. Pp. 30–34. (In Russian)
15. Mitra D., Ramakrishman K.G. Technics for traffic engeniring of multiservice in priority networks. *BLTJ*. 2001. Vol. 1. Pp. 123–130.
16. Zima V.M., Moldovyan A.A., Moldovyan N.A. *Bezopasnost' global'nyh setevyh tehnologij* [The global security network technologies]. St. Petesburg: SPbU, 1999. 234 p. (In Russian)
17. Kotenko I.V., Stepashkin M.V., Bogdanov V.S. Vulnerability Analysis of Computer Networks on Design Stages and Maintenance. Izvestiya vysshikh uchebnykh zavedeniy. *Priborostroenie* [Journal of Instrument Engineering]. 2006. Vol. 49. No. 5. Pp. 3–8. (In Russian)
18. Gorodetsky V., Kotenko I., Karsayev O. The Multiagent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. *The International Journal of Computer Systems Science &Engineering*. 2003. Vol. 18. No. 4. Pp. 191–200.
19. Harmer P., Williams P., Gunsch G., Lamont G.B. An artificial immune system architecture for computer security applications. *IEEE Transactions on Evolutionary Computation*. 2002. Vol. 6. No. 3. Pp. 252–280.
20. Al-Kasassbeh M., Adda M. Network fault detection with Wiener filter-based agent. *Journal of Network and Computer Applications*. 2009. Vol. 32. No. 4. Pp. 824–833.

INFORMATION ABOUT AUTHORS:
Burenin A. N., PhD, Full Professor, Chief specialist of "Research Institute "Rubin";
Legkov K. E., PhD, Head of the Department of automated systems of control of the Military Space Academy;
Pervov M.S., Military academy of communication of Marshall of the Soviet Union S. M. Budenny.

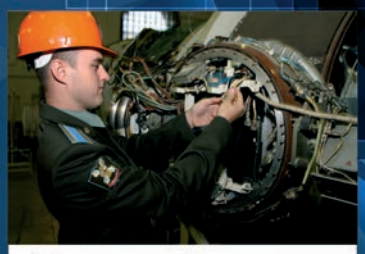
For citation: Burenin A.N., Legkov K.E., Pervov M.S. The organization of procedures for identification and localization of violations of security policies at security management of functioning of a subsystem of providing with uniform time of the automated control system for a complex organizational and technical system. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 28–36. doi: 10.24411/2409-5419-2018-10185 (In Russian)



КРУПНЕЙШИЙ ПОЛИТЕХНИЧЕСКИЙ ВУЗ ВС РФ
ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Обучение в Санкт-Петербурге

Высокий социальный статус



Огромный выбор специальностей

Повышенная стипендия

Высокооплачиваемая работа

Обеспечение питанием и форменной одеждой

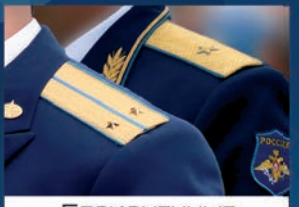
Проживание в общежитии

Престижные профессии будущего

Гарантированное трудоустройство

Востребованность в Вооруженных силах РФ

Романтика военной службы



Бесконечные возможности карьерного роста и социальный лифт

ИНФОРМАЦИЯ ДЛЯ ПОСТУПАЮЩИХ

Почтовый адрес: 197198, г. Санкт-Петербург,
ул. Ждановская, д. 13.
Телефоны приемной комиссии: (812) 347-96-59, 347-97-70.
Факс: (812) 237-12-49.
Сайт: www.mil.ru, www.academy-mozhayskogo.ru
Адрес электронной почты: spb.vka@yandex.ru.

doi: 10.24411/2409-5419-2018-10186

МЕТОД PROCESS MINING В СИСТЕМЕ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

ВАСИЛЬЕВ
Николай Владимирович[1]

ЗАБРОДИН
Олег Вадимович[2]

КУЛИКОВ
Дмитрий Вадимович[3]

АННОТАЦИЯ

Предложен метод анализа журналов событий системы электронного документооборота, основанный на методологии Process Mining (глубинный анализ процессов), позволяющий осуществить реконструкцию проекции потока управления, проекции ресурсов и проекции данных рабочих процессов обработки документов на предприятии. Метод основывается на анализе журналов действий над документами. Предполагается, что на предприятии ставится «пустая» система без описаний рабочих процессов и пользователи выполняют привычные действия в ручном режиме. После обработки нескольких однотипных документов журнал становится «полным», что позволяет реконструировать предполагаемый процесс обработки документа. После рецензии полученного процесса аналитиком и внесения изменений, процесс может быть загружен в систему и назначение прохождения всех инстанций документом будет автоматизировано. В рамках исследования предлагается следующая схема реконструкции перечисленных проекций процесса документооборота: сегментирование журнала событий по типам документов; сегментирование полученных журналов по стадиями жизненного цикла документа; реконструкция проекции потока управления; реконструкция проекции ресурсов; реконструкция проекции данных и принятия решений. Необходимость первого шага обусловлена тем, что с одним типом документов в журнале могут быть связаны несколько типов рабочих процессов. Второй шаг позволяет отделить трассы событий различных процессов обработки одного типа документов. Разбиение производится на основе стадий жизненного цикла типа документа. После выделения множества трасс на следующем шаге проводится реконструкция проекции потока управления рабочего процесса модифицированным альфа-плюс алгоритм, позволяющим получать в качестве результата схему процесса. На следующем шаге для обеспечения реконструкции проекции ресурсов используется дерево организационно-штатной структуры предприятия, в котором промежуточные узлы – подразделения организации и должности, а листья – должностные лица. Реконструкция осуществляется на основе предложенных эвристических правил. Реконструируемая на следующем шаге проекция данных, описывающая основные атрибуты экземпляра процесса соответствует регистрационной карточке документа. В работе предложена процедура выявления делегатов управления поведением исключающих шлюзов процесса. Для каждого исключающего шлюза, полученного при реконструкции модели управления потоком по журналу, строится пара предикатов на выражениях сравнений атрибутов регистрационной карточки. Указанные предикаты вычисляются алгоритмом автоматического построения деревьев решений. Приведенные выше методы реконструкции проекций моделей процессов были реализованы в виде компонента в составе BPMN – редактора процессов документооборота.

КЛЮЧЕВЫЕ СЛОВА: анализ процессов; документооборот; бизнес-процесс; принятие решений; альфа-плюс алгоритм; жизненный цикл документа; анализ журналов событий.

Сведения об авторах:

[1]к.т.н., начальник сектора публичного акционерного общества «Интелтех», г. Санкт-Петербург, Россия, gandvik1984@gmail.com

[2]инженер публичного акционерного общества «Интелтех», г. Санкт-Петербург, Россия, olegzabrodin@gmail.com

[3]инженер публичного акционерного общества «Интелтех», г. Санкт-Петербург, Россия, dima_kulikov1993@mail.ru

Для цитирования: *Васильев Н. В., Забродин О.В., Куликов Д.В.* Метод Process Mining в системе защищенного электронного документооборота // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 38–50. doi: 10.24411/2409-5419-2018-10186

В современном мире подавляющий объём информации существует в электронном виде. Для хранения, обработки и управления документами на цифровых носителях широкое распространение получили системы электронного документооборота (СЭД), представляющие собой автоматизированные многопользовательские системы, сопровождающие процесс создания и перемещения по организации документов.

Большинство современных СЭД строится на основе процессного подхода, в соответствии с которым документооборот промышленного предприятия или государственного ведомства представляется в виде формализованного множества описаний последовательности выполняемых сотрудниками операций над документами.

Однако, внедрение подобной системы приводит к чрезмерному увеличению нагрузки на аналитиков и сотрудников служб обеспечения. Это связано с необходимостью формализации процессов движения документов на предприятии. Особенно сложной эта задача становится при изменении структуры организации, штатной численности или при переориентации деятельности предприятия. Вследствие описанных структурных изменений имеющаяся модель процессов теряет актуальность. Порой степень несоответствия модели процессов приводит к необходимости разработки моделей процессов «с нуля».

Актуальность темы работы обусловлена тем, что в настоящий момент в составе СЭД отсутствуют средства, позволяющие автоматизировать процесс создания и корректировки моделей процессов обработки документов на предприятии.

Большинство современных СЭД поддерживают журнализацию действий пользователей. В последние годы в зарубежных [1] и отечественных [2] работах получило развитие направление, носящее название «Глубинный анализ процессов» (*Process Mining*), которое позволяет на основе журналов событий информационных систем реконструировать схемы рабочих процессов (*workflow*), реализуемые пользователями. Однако в настоящее время данные средства в системах электронного документооборота пока еще не получили широкого распространения.

В работе предпринята попытка разработки инфраструктуры глубинного анализа процессов в структуре защищенного электронного документооборота. Предложенные модели и методы были реализованы в прототипе модуля, позволяющего помочь интеграторам СЭД при решении задачи создания и актуализации бизнес-процессов документооборота предприятия.

Приводится общая характеристика современных систем документооборота, приведен разработанный метод глубинного анализа процессов в СЭД и описан разработанный прототип модуля анализа процессов, реализующий предложенный метод.

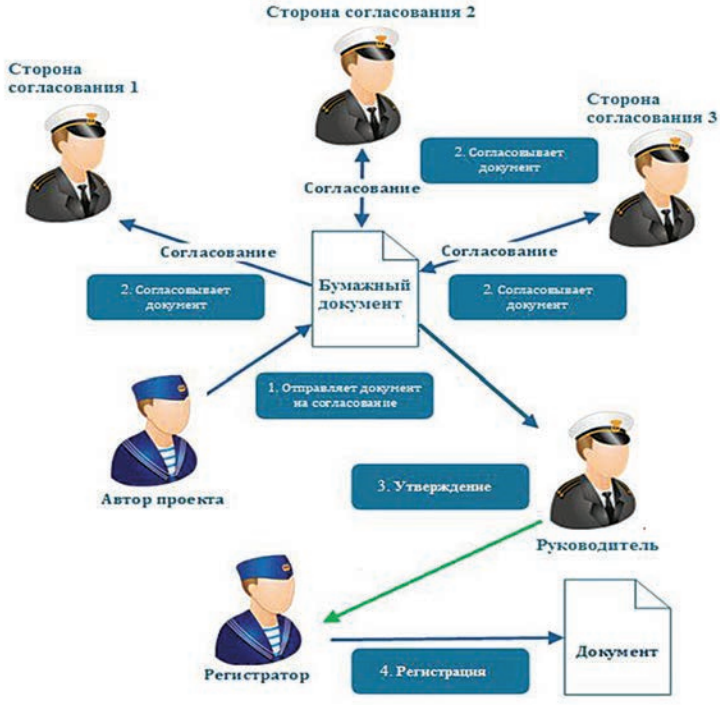
Характеристика современных систем электронного документооборота

За последние 20 лет концепция электронного документооборота получила свое развитие от идеи сканирования и централизованного хранения графических образов документов до идеи управления документами и их карточками от момента создания до регистрации, подписи и сдачи в архив. Необходимость решения задачи маршрутизации документов внутри организации между исполнителями привела к внедрению в СЭД технологии рабочих (бизнес) процессов (БП). СЭД также решают задачу интеграции всех информационных приложений в единую информационную среду, обеспечивающую оперативное взаимодействие всех пользователей при выполнении ими деловых процедур и функций управления необходимой информацией. Русский термин «системы электронного документооборота» является некорректным, так как основным объектом хранения СЭД выступают не документы, а регистрационно-учетные карточки. Документ при этом может храниться в базе данных СЭД, файловой системе или в бумажном виде на полке в папке. В этом отношении англоязычный термин *EDRMS* (*Electronic Document Record Management Systems*) является более правильным.

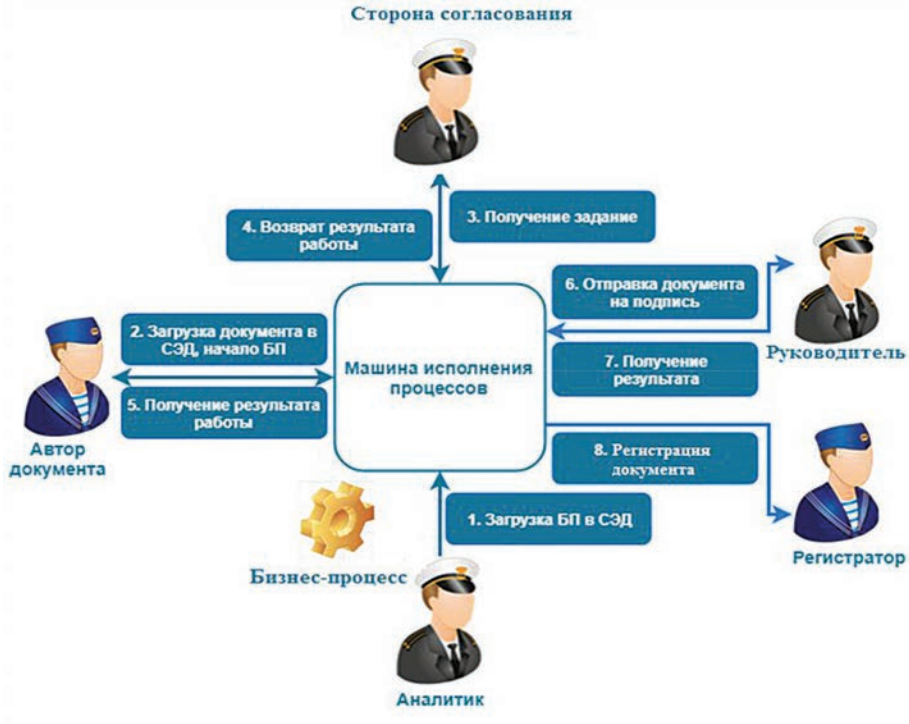
Современные СЭД условно можно разделить на 2 класса: документ — ориентированные (*docflow*) и процесс — ориентированные (*workflow*) СЭД. Основой как первого так и второго класса СЭД является подход на основе рабочих процессов. Пример автоматизации деятельности сотрудников на примере процесса огласования документа представлен на рис. 1.

Организация рабочих процессов в *docflow* — СЭД идет от документа. Для каждого документа, прошедшего систему, создается задача (экземпляр рабочего процесса). Рабочие процессы имеют в *docflow* — СЭД общий характер, и, как правило, соответствующее название «Согласование», «Утверждение», «Рассмотрение». В то время как в *workflow* — СЭД с одним экземпляром рабочего процесса могут быть связаны несколько документов. Процессы в этом случае носят специфический характер и название: «Обслуживание заявки на подключение клиента», «Проведение сделки», «Аттестация персонала» и пр. Безотносительно типа СЭД задачи размещаются на сервере баз данных. Задачи характеризуются статусом (выполнена/в процессе/просрочена), прикрепленными документами, маршрутом движения документа, списком пользователей-исполнителей, а также временными параметрами.

Как правило, в СЭД каждый документ характеризуется типом, а тип в свою очередь моделью жизненного цикла. Жизненный цикл определяет, какие стадии и в каком порядке может проходить документ. Например, практически все документы проходят стадии разработки, согласования и утверждения, а также списания в архив.



а



б

Рис. 1. Пример согласования документа в ручном режиме (а) и средствами системы электронного документооборота (б)

Для специфических типов документов могут выделяться специфические стадии.

Современные СЭД [3–4] строятся на основе реляционных баз данных. Более близкая к СЭД концепция документ — ориентированных *NoSQL* — баз данных не получила пока широкого распространения. Идеологически, в составе СЭД можно выделить набор сервисов:

– *сервис справочников*, предназначенный для хранения условно-постоянной информации, используемой пользователями СЭД при работе с документами;

– *сервис пользователей*, предназначенный для управления пользователями и разграничения прав доступа. Он отвечает за авторизацию и аутентификацию пользователей системы по доступу к папкам и файлам, для чего использует как механизмы клиентской составляющей системы, так и встроенные механизмы безопасности базы данных;

– *сервис поиска и индексации*, предназначенный для реализации механизмов полнотекстового поиска. Сервис производит периодическую индексацию таблиц документов и справочников с сохранением индекса в специальной таблице или на диске;

– *объектные сервисы*, реализующие базовые операции создания, чтения, обновления и удаления (*CRUD*) над объектами, включая документы, справочники, задачи и задания рабочих процессов. Для объектов — документов это включает установку и получение свойств и потоков содержимого файлов;

– *сервис каталогов*, осуществляющий доступ к объектам, размещаемым в иерархии папок путем добавления или удаления объектов из папки. Папки могут содержать другие папки и документы;

– *сервис исполнения рабочих процессов*, служащий для создания новых экземпляров рабочих процессов документооборота, генерации и назначения заданий исполнителям, поддержки и контроля выполнения созданных экземпляров. Данный сервис использует для своей работы все перечисленные выше сервисы.

Как показано на рис. 2 описание рабочего процесса документооборота может быть представлено как набор из 4 проекций-перспектив.

Перспективе «*управление потоком*» соответствует маршрут движения документа между исполнителями (схема рабочего процесса).

Перспективе «*данные*» соответствует документ, над которым выполняется экземпляр процесса, а также набор дополнительных переменных процесса (переменных управления).

Перспективе «*ресурсы*» соответствует набор ролей и исполнителей, которые могут выполнять действия над документом в узлах схемы рабочего процесса.

Перспективе «*операции*» соответствует список элементарных действий, совершаемых исполнителями с документом в рамках задания. Например, скачать документ, подписать документ, создать новую версию, перенести в другую папку и пр.

Рис. 2. Проекции модели рабочего процесса

В существующей схеме создание и загрузку рабочих процессов в СЭД в виде файлов BPMN (*Buisness process management notation*) производит администратор с помощью редактора [5]. Подобная схема в силу субъективности и неточности имеет недостатки. В работе далее предлагается метод, который позволяет частично их устранить.

Process Mining в системе электронного документооборота

Привлечение Process Mining вносит в привычную схему развертывания бизнес-процессов документооборота коррективы. На предприятие ставится система с минимально необходимым набором процессов и пользователи выполняют привычные действия в ручном режиме. Например, при согласовании документа вручную указывают все согласующие инстанции, которые должен пройти данный документ. В процессе согласования факты выполнение всех действий заносятся в журнал. После обработки нескольких однотипных документов журнал становится «полным», что позволяет реконструировать предполагаемый процесс обработки документа. То есть после рецензии полученного процесса аналитиком и внесения изменений процесс может быть загружен в систему и движение документа по организации будет автоматизировано.

Согласно [1–8] для обеспечения реконструкции схемы процесса журнал событий должен иметь как минимум четыре атрибута:

– действие (*activity*) — действие, выполненное пользователем например, «подпись документа», «наложение резолюции»;

– время регистрации (*timestamp*) — момент времени, когда произошло события;

– идентификатор последовательности событий (*case id*) — идентификатор последовательность действий над определенным документом;

– ресурс (*resource*) — исполнитель, или инициатор действия пользователь или внешняя информационная система).

В рамках СЭД отдельный экземпляр рабочего процесса ассоциируется с документом, поэтому трассы могут быть выявлены по идентификатору документа, который соответствует идентификатору последовательности (*case id*) рассмотренного журнала. Общая схема метода реконструкции рабочих процессов документооборота показана на рис. 3.

Необходимость шагов 1–2 обусловлена тем, что с одним типом документов в журнале могут быть связаны несколько рабочих процессов, поэтому важно определить признак, по которому трассы одного процесса отличаются от трасс другого. Это может быть сделано исходя из положения, что каждый документ имеет свой *тип*, а тип в свою очередь характеризуется *жизненным циклом*. Жизненный цикл (ЖЦ) документа — тип поведения документа от момента формирования до момента передачи в архив (на хранение) или уничтожения.

Жизненный цикл может быть описан в форме графа, в котором вершинами являются стадии жизненного цикла, а ребрами — переходы между стадиями. При выделении трасс рабочего процесса можно исходить из принадлежности действий к одной стадии ЖЦ. К одному рабочему процессу могут быть отнесены трассы от момента начала до момента окончания стадии ЖЦ. Например, на приведенной на рис. 4 схеме, к рабочему процессу «Согласование документа» будут отнесены все трассы, ведущие из стадии ЖЦ документа «Согласование» (т.е. «документ в процессе согласования») к стадии «Исполнение» и из «Согласование» в «Прекращен». А для процесса «Исполнение документа» все трассы ведущие из стадии ЖЦ документа «Исполнение» в «Исполнен» или «Прекращен».

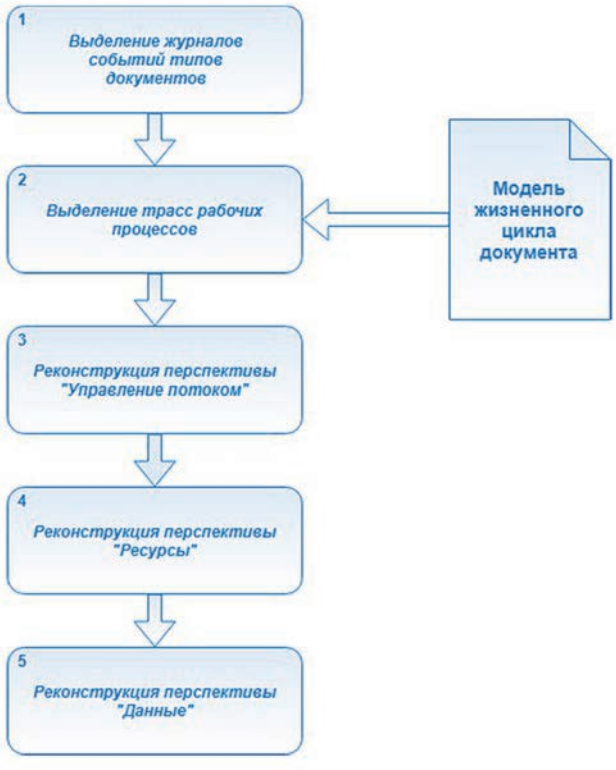


Рис. 3. Схема процесса реконструкции рабочих процессов документооборота

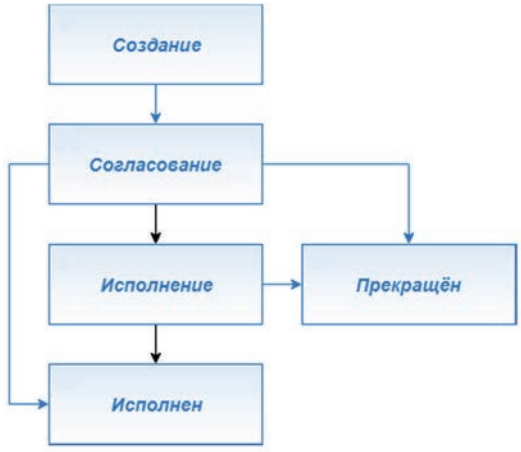


Рис. 4. Пример жизненного цикла типа документа

Жизненный цикл каждого типа документа должен быть описан. В разработанном прототипе для этих целей был использован справочник «Жизненный цикл документа», связанный со справочником «Типы документов».

После выделения множества трасс может быть проведена реконструкция перспективы «Поток управления» рабочего процесса одним из алгоритмов Process Mining (шаг 3 на рис. 3). При разработке прототипа был использован альфа-плюс алгоритм [9]. Общая схема реконструкции проекции «Поток управления» показана на рис. 5.

Алгоритм на первом этапе на основе журнала событий строит матрицу пар отношений между событиями. Выделяется 4 типа отношений:

– прямая преемственность $(a >_L b)$ — шаблонное отношение, наблюдающееся, когда в журнале событий присутствует хотя бы одна трасса, в которой событие b следует сразу же за событием a;

– причинность $(a \rightarrow_L b)$ — отношение наблюдается в журнале только когда есть хотя бы одна трасса, где $(a >_L b)$ и нет ни одной трассы, в которой $(a \not\succ_L b)$. То есть можно говорить, что причиной появления события b в журнале служит событие a;

– несвязность $(a \#_L b)$ — шаблонное отношение, наблюдаемое, когда в журнале $(a >_L b)$ и $(b >_L a)$

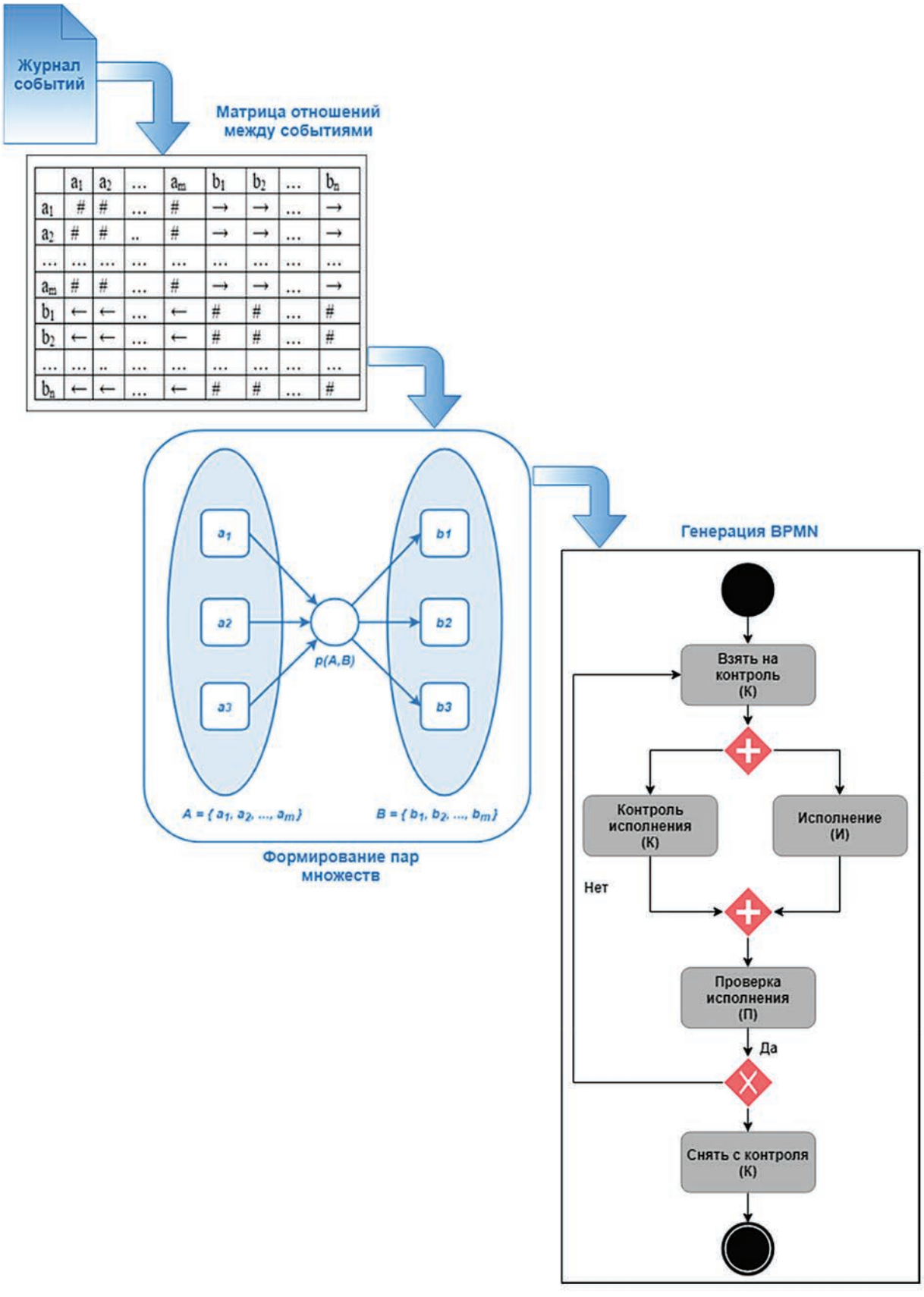


Рис. 5. Схема реконструкции модели потока управления

– параллельность $(a \|_L b)$ — отношение, наблюдаемое в журнале, если $(a \succ_L b)$ и $(b \succ_L a)$.

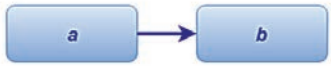
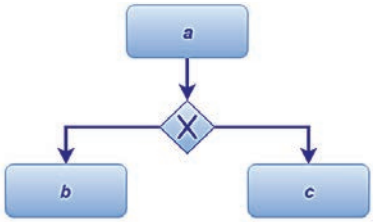
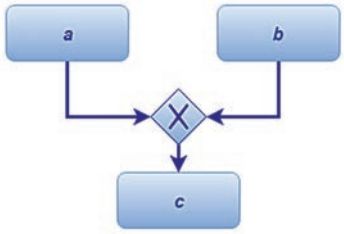
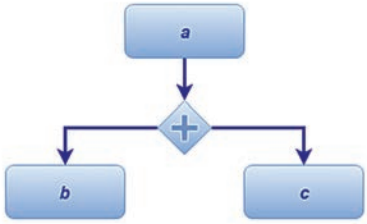
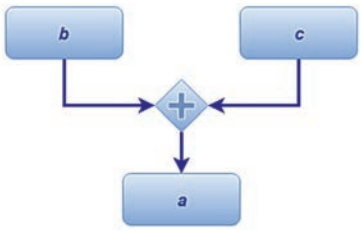
На втором этапе множество событий разбивается на пары множеств (*A*, *B*) по следующему принципу: каждый элемент множества *A* связан с каждым элементом множества B, при этом внутри *A* и *B* события связаны отношением '#' (несвязность).

Базовая версия альфа-плюс алгоритма использует в качестве целевого представления сеть Петри. Переход к нотации *BPMN* на третьем этапе был осуществлен при помощи таблицы преобразования (табл. 1).

Проекция «Операции» (см. рис. 2) поддерживается на уровне системы электронного документооборота и может в себя включать такие элементарные действия над

Таблица 1

Условия для генерации фрагментов нотации BPMN на основе альфа-алгоритма

Фрагмент в нотации BPMN	**Последовательное выполнение**
Последовательное выполнение 	присутствует пара (A, B) $a \in A, b \in B$, не выполняются другие условия
Условное разделение 	присутствует пара (A, B) $a \in A$, $b \in B, c \in B$
Условное слияние 	присутствует пара (A, B) a ∈ A, b ∈ A, c ∈ B. не выполняются другие условия
Параллельное разделение 	$a \in A_1, a \in A_2, b \in B$, $c \in C$ и присутствуют пары отношений (A_1, B) (A_2, C)
Параллельное слияние 	$a \in A_1, a \in A_2$, $b \in B$, $c \in C$ и присутствуют пары отношений (B, A_1) (C, A_2)

документом как: изменение, просмотр, подписание, блокировка, создание и удаление версии. Исполнение каждого действия сопровождается занесением записи в журнал. Кроме этого в модель операций должны быть включены действия исполнителей с данными регистрационных карточек. Предполагается, что в качестве одного действия результирующего журнала рассматривается набор действий по изменению атрибутов карточки, выполняемых последовательно одним пользователем.

На шаге 4 (см. рис. 3) для обеспечения реконструкции проекции «Ресурсы», т.е. модели исполнителей процесса в журнале должно содержаться поле «Исполнитель действия». Указанное поле может быть взято из справочника «Пользователи». Реконструкция роли исполнителя действия может быть осуществлена на основе связанных справочников «Должностные лица» (ДЛ), «Должности» (Д) и «Подразделения организации» (ПО). На основе указанных справочников формируется дерево, в котором промежуточные узлы — подразделения организации и должности, а листья — должностные лица (рис 6).

Назначение исполнителей заданий рабочих процессов может быть осуществлена на основе следующих эвристических правил:

если на множестве трасс действия всегда исполняет одно и то же должностное лицо, то роль может соответствовать только этому ДЛ;

в случае если исполнителем действия выступают разные должностные лица, в качестве роли может быть использован промежуточный узел дерева (наименьшее по численности подразделение или должность), включающий в качестве потомков всех указанных ДЛ.

Рассмотрим заключительный шаг 5 метода (см. рис. 3). В случае электронного документооборота, перспектива «Данные», описывающая основные атрибуты

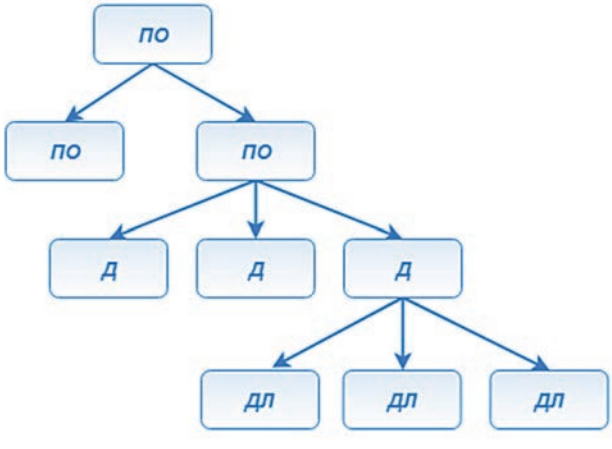


Рис. 6. Фрагмент дерева организационно-штатной структуры для реконструкции перспективы «Ресурсы»

экземпляра процесса содержится в регистрационной карточке. Карточка, наряду с жизненным циклом описаны в справочнике «Тип документа» куда заносится администратором СЭД. Для заполнения регистрационной карточки используются следующие базовые типы атрибутов: «Дата», «Дробное число», «Признак», «Справочник», «Строка», «Текст», «Целое число».

В разных действиях рабочего процесса документооборота исполнители работают с различными подмножествами атрибутов регистрационной карточки. Как было отмечено, под одним действием предполагается набор изменений реквизитов карточки, выполняемых последовательно одним пользователем.

Полнота описания перспективы «Данные» также обеспечивается заданием модели поведения исключающих шлюзов. То есть условий заданных на значениях реквизитов карточки в зависимости от которых срабатывают исключающие шлюзы, соответствующие условным переходам процесса (рис. 7). Каждый вариант прохождения исключающего шлюза представлен отдельной трассой в журнале событий. Таким образом, для каждого исключающего шлюза, полученного при реконструкции модели управления потоком по журналу должна быть построена пара предикатов вида:

$$(атрибут_1\ оп.сравн.\ значение_1)\ \text{ИЛИ}$$
$$(атрибут_2\ оп.сравн.\ значение_2)\ \text{ИЛИ}\ldots,$$

где *оп.сравн.* — операции сравнения: «>», «<», «=».

Каждое из полученных выражений определяет вариант исполнения исключающего шлюза.

Данное построение может быть выполнено алгоритмом автоматического построения деревьев решений C4.5 (см. напр. [10]). Метками классов, соответствующих листьям дерева принятия решений соответствуют пары событий до и после условного перехода (см. рис. 7). Однако реализация для перечисленного набора типов данных налагает свои особенности:

– для атрибутов типа «Признак» и «Справочник» алгоритм используется без модификаций. В процессе построения дерева решений для каждого возможного значения признака или записи справочника создается отдельное поддерево;

– для атрибутов «Целое число» и «Дробное число» производится дискретизация. Для каждого численного реквизита определяется возможный размах значений с последующим разбиением на интервалы — по одному для каждого поддерева;

– на множестве атрибутов типа «Дата» вычисляются все возможные разности (целые числа), после чего задача сводится к классификации целочисленных значений;

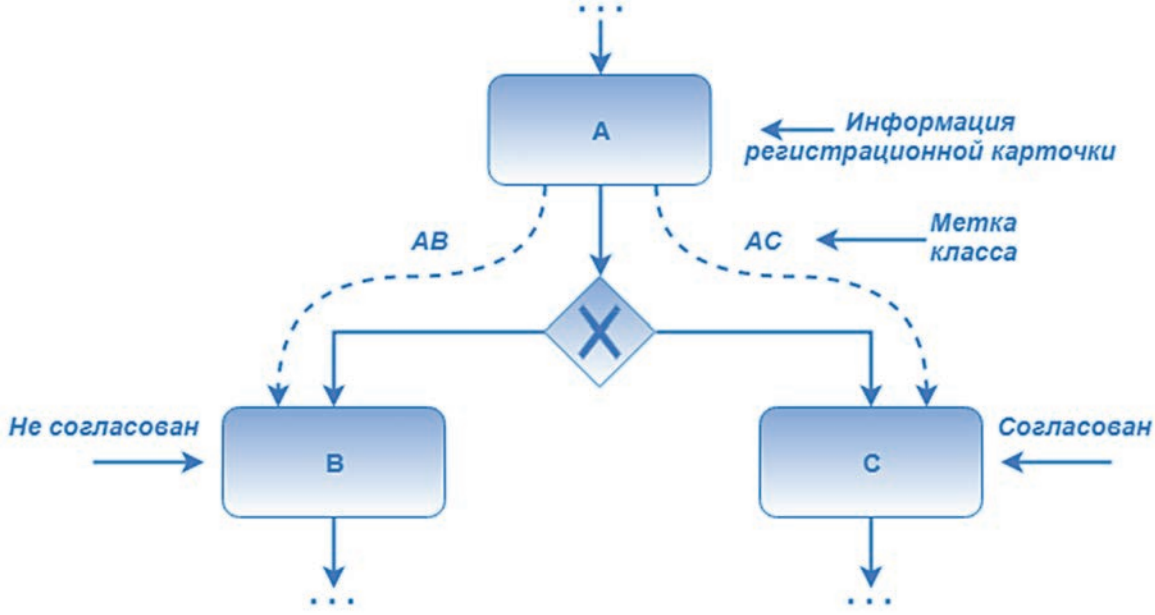


Рис. 7. Схема срабатывания условного перехода в рабочем процессе с меткой класса маршрута

– на множестве значений реквизитов типа «Строка» и «Текст» выполняется индексирование и последующее ранжирование алгоритмом *PageRank* (см. [11]) с формированием групп связанных между собой значений. Данные группы соответствуют поддеревьям узла текстового реквизита.

Рассмотрим пример построения схемы принятия решений (табл. 2). Из регистрационной карточки было взято два атрибута «Срок исполнения» и «Поле резолюции» (X_1 и X_2). Первое поле относится к типу «Дата», а второе имеет тип «Текст». Для дальнейшего анализа было введено поле $X_1^{//}$ и $X_2^{//}$. Первое представляет разницу между сроком выполнения и текущей датой (10.10.2018) в днях, а во втором хранится отношение резолюции к одной из групп: possitive(положительное решение), negative (отрицательное решение), *null group* (без резолюции). Данное отношение было получено с использованием алгоритма ранжирования (см. [11] и табл. 2). Вариант прохождения исключающего шлюза указан в виде столбца *Y*. На данном наборе данных было построено дерево принятия решений (рис. 8) по алгоритму C4.5. На каждом шаге алгоритм последовательно вычисляет энтропию и прирост информации (см. подробнее [10]) для каждого атрибута регистрационной карточки. Выбор атрибута для текущего узла дерева решения производится на основе критерия максимизации прироста информации. Энтропия приведенного фрагмента до разбиения равна 0,9852.

Энтропия при разбиении по атрибуту $X_1^{//} = 0{,}3935$.

Прирост информации по атрибуту $X_1^{//} = 0{,}5917$.

Энтропия при разбиении по $X_2^{//} = 0{,}6935$.

Прирост информации по $X_2^{//}$=0,2916

Таким образом на основе приведенного критерия на первом шаге для ветвления должен использоваться $X_1^{/}$. Фрагмент построенного дерева показан на рис. 8.

Построенные предикаты в виде делегатов хранится в описании рабочего процесса и ассоциируется с конкретным шлюзом.

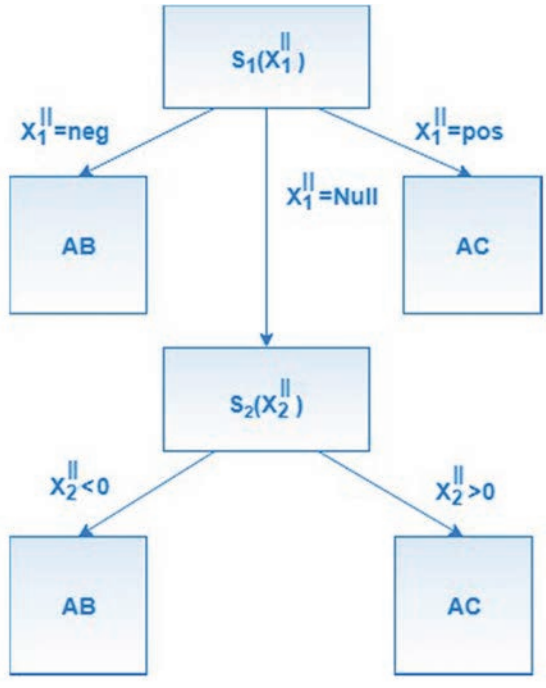


Рис. 8. Пример дерева принятия решений

Таблица 2

Реквизиты фрагмента регистрационной карточки для реконструкции дерева решений

X_1	X_2	$X_1^{//}$	$X_2^{//}$	Y
20.10.2018	Изменить название пункта 2.2	*neg* (изменить)	9	*AB*
18.10.2018	В приказе добавить подпись Иванова В.В.	*neg* (добавить)	7	*AB*
15.10.2018	Приказ одобрен. Для ознакомления	*pos* (одобрено)	4	*AC*
09.10.2018	Null	*Null*	-1	*AB*
11.10.2018	Null	*Null*	1	*AC*
12.10.2018	На счет правок невозрожаю.	*pos* (невозражаю)	2	*AC*
01.10.2018	Не смотрел	*Null*	-9	*AB*

Реализация инфраструктуры анализа процессов в СЭД

Предложенный метод реконструкции проекций моделей процессов был реализованы в виде компонента в составе редактора рабочих процессов документооборота «Цера» [12]. Отличительной особенностью разработанного модуля от уже существующих решений (см. напр. [13–15]) является ориентация на анализ процессов документооборота.

Инфраструктура *Process Mining* в СЭД показана на рис. 9. В процессе функционирования редактор обращается к базе данных и справочникам документооборота. На первом этапе модулем построения модели управления потоком осуществляется процесс сегментирования журнала собы-

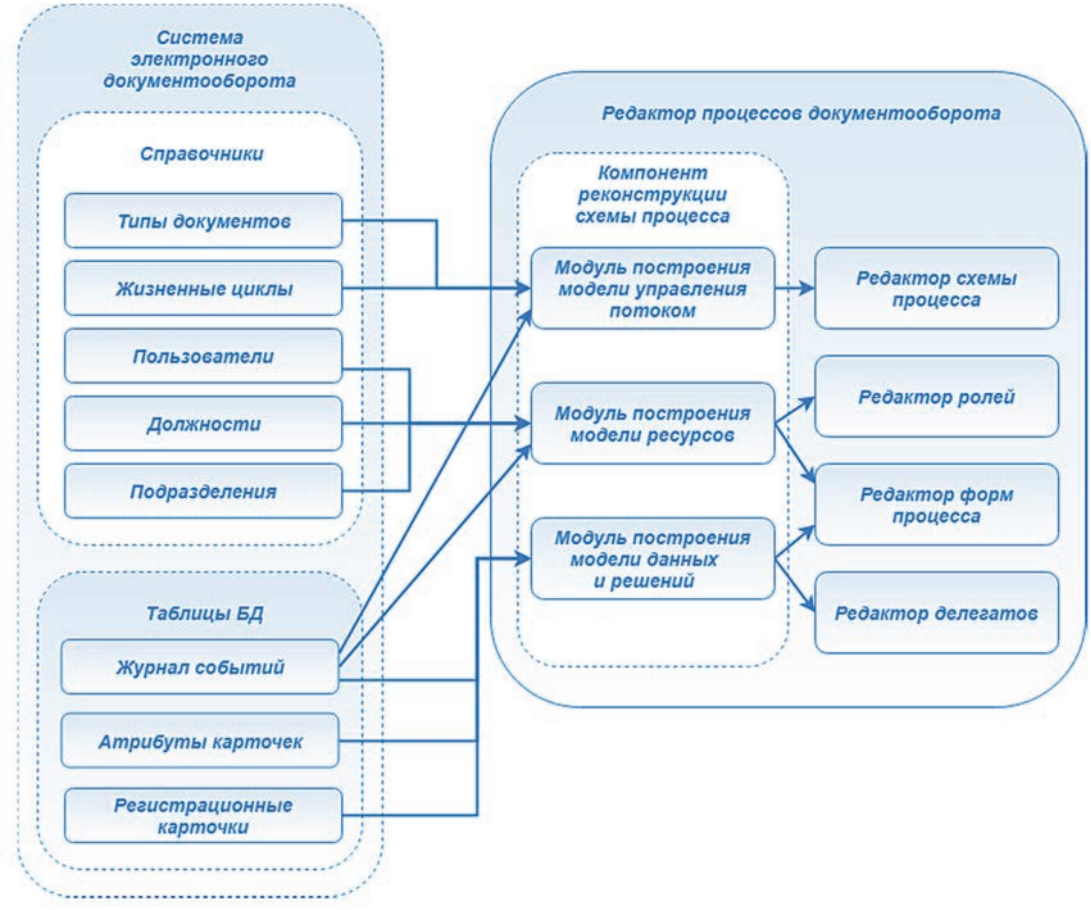


Рис. 9. Инфраструктура Process Mining в системе электронного документооборота

тий на основе выбранного пользователем типа документа и стадии его жизненного цикла. После чего производится реконструкция BPMN — графа рабочего процесса. На основании рассмотренной методики модуль построения модели ресурсов производит обращения к справочникам описания организационно-штатной структуры и последующее назначение ролей заданиям схемы рабочего процесса.

Дальнейшую работу выполняет модуль построения модели данных и решений, производящий на основе таблиц «Регистрационная карточка» и «Атрибут карточки», а также json-поля «образ атрибутов» таблицы «Журнал событий» производит создание форм заданий рабочего процесса, а также формирование предикатов для делегатов, обеспечивающих поведение исключающих шлюзов.

Практическая апробация разработанного модуля показала недостаточную эффективность альфа — плюс алгоритма для решения задач анализа реальных журналов СЭД. В случае наличия ошибок в журнале (дублирование или выпадение событий, ошибки ручного выполнения операций) авторами были получены слабо читаемые модели, объем ручных модификаций которых по доводке до рабочих процессов был значителен. В качестве дальнейших исследований авторы предполагают использовать алгоритм индуктивного анализа (Inductive miner), позволяющий, как и альфа-плюс алгоритм создавать бездеффектное (soundness) описание процессов, но не столь чувствительные к ошибкам (см. напр. [15]). Была также определена зависимость результатов анализа от дисциплинированности исполнителей документов, на основе которых действий которых формируется исходный журнал. В случае несвоевременного указания значений реквизитов регистрационной карточки при выполнении действий наблюдалась некорректная проекция данных процесса. В качестве частичной меры преодоления указанного недостатка авторами предлагается привязка групп реквизитов регистрационной карточки к стадиям ЖЦ типа документа. Открытым остается также вопрос оценки степени деградации схемы рабочего процесса при организационно-штатных и нормативных изменениях на предприятии.

Литература

1. *Van der Aalst W.M.P.* Process Mining: Discovery, Conformance and Enhancement of Business Processes. Berlin: Springer-Verlag, 2011. 352 p.

2. *Барсегян А. А., Куприянов М.С., Холод И.И., Тесс М.Д., Елизаров С.И.* Анализ данных и процессов. СПб.: БХВ-Петербург, 2009. 512 с.

3. *Романченко Е.В.* Основные тенденции развития СЭД в России // Современные технологии делопроизводства и документооборота. 2015. № 8. URL: http://e.deloprost.ru/article.aspx?aid=419473 (дата обращения 05.10.2018).

4. *Мокрый В.Ю.* Системы электронного документооборота. СПб.: Инфо-да, 2018. 48 с.

5. *Михеев А.Г.* Системы управления бизнес-процессами и административными регламентами на примере свободной программы RunaWFE: учеб. Пособие. Москва: Альт Линукс, 2011. 178 с.

6. *Van der Aalst W.M.P., Weijters A.J.M.M., Maruster L.* Workflow Mining: Discovering process models from event logs // IEEE Transactions on Knowledge & Data Engineering. 2004. Vol. 16. No. 5. Pp. 1128–1142.

7. V*an der Aalst W.M.P., van Dongen B.F.* Discovering Workow Performance Models from Timed Logs // EDCIS2002: Engineering and Deployment of Cooperative Information Systems. LNCS. Berlin: Springer, 2002. Vol. 2480. Pp. 45–63.

8. *Van der Aalst W.M.P., Weijters A.J.M.M.* Process mining: a research agenda // Computers in Industry. 2004. No. 53(3). Pp. 231–244.

9. *De Medeiros A.K. A, van Dongen B.F., van der Aalst W.M.P., Weijters A.J.M.M.* Process Mining: Extending the α-algorithm to Mine Short Loops / Eindhoven University of Technology, Eindhoven, 2004. URL: https://pure.tue.nl/ws/files/1864325/576199.pdf (дата обращения 05.10.2018).

10. *Паклин Н.Б., Орешков В.И.* Бизнес-аналитика: от данных к знаниям. СПб.: Питер, 2009. 624 с.

11. *Марманис Х., Бабенко Д.* Алгоритмы интеллектуального интернета. Передовые методики сбора, анализа и обработки данных. СПб.: Символ-Плюс, 2011. 480 с.

12. Свидетельство о регистрации программы для ЭВМ 2017663083. Российская Федерация. Подсистема защищенного электронного документооборота «Цера» / Васильев Н.В., Компанец А.Н., Сопин Д.С. Заявитель и правообладатель ПАО «Интелтех» (RU). Заявл. 06.10.17; Опубл. 24.11.17. Реестр программ для ЭВМ. 1 с.

13. *Van Dongen B., de Medeiros A., Verbeek H., Weijters A., van der Aalst W.M.P.* The prom framework: A new era in process mining tool support // ICATPN2005: Applications and Theory of Petri Nets. LNCS. Springer, 2005. Vol. 3536. Pp. 444–454.

14. *Van Dongen B.F., van der Aalst W.M.P.* EMiT: A Process Mining Tool // ICATPN2004: Applications and Theory of Petri Nets. LNCS. Springer, 2004. Vol. 3099. Pp. 454–463.

15. *Leemans S.J.J., Fahland D., van der Aalst W.M.P.* Discovering Block-Structured Process Models from Event Logs — A Constructive Approach // Petri Nets. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013. Vol. 7927. Pp. 311–329.

PROCESS MINING METHODS IN THE SECURE ELECTRONIC DOCUMENT CONTENT RECORD MANAGEMENT SYSTEMS

NICKOLAY V. VASILIEV
Saint-Petersburg, Russia, gandvik1984@gmail.com

OLEG V. ZABRODIN
Saint-Petersburg, Russia, olegzabrodin@gmail.com

DMITRY V. KULIKOV
Saint-Petersburg, Russia, gandvik1984@gmail.com

KEYWORDS: Process mining; electronic document record management systems; decision support; alpha- algorithm; document life cycle; event log analysis.

ABSTRACT

The work proposes a process mining method for analysis of EDRMS workflow processes. The method is based on the analysis of document action logs. It is assumed that an "empty" system is put in the enterprise without descriptions of workflows and users perform familiar actions in manual mode. After processing several documents of the same type, the journal becomes "complete", which allows reconstructing the intended document processing process. After reviewing the received process by the analyst and making changes, the process can be loaded into the system and the appointment of the passage of all instances by the document will be automated. The study proposes the following scheme for the reconstruction of the listed projections of the BPMN model – the workflow process: event log segmentation by document type; segmentation of received logs by stages of the document life cycle; reconstruction of the control flow projection; reconstruction of the projection of resources; reconstruction of data projection and decision making. The need for the first step is due to the fact that several types of workflows can be associated with a single type of document in a journal. The second step allows you to separate the event traces of processing a single document. The splitting is based on the life cycle stages of the document type. After selecting a set of traces, in the next step, the projection of the workflow control flow of the modified alpha-plus algorithm is reconstructed, which allows to obtain a BPMN-graph of the process as a result. In the next step, to ensure the reconstruction of the projection of resources, the tree of the organizational structure is used, in which the intermediate nodes are organizational units and positions, and the leaves are officials. Reconstruction is carried out on the basis of the proposed heuristic rules. The data projection reconstructed in the next step, describing the main attributes of the process instance, corresponds to the registration card of the document. The paper proposes a procedure for identifying delegates for controlling the behavior of exclusive process gateways. For each exclusive gateway, obtained during the reconstruction of the flow control model according to the log, a pair of predicates is built on expressions of comparisons of the attributes of the registration card. The construction of these predicates was performed by an algorithm for the automatic construction of decision trees. The above methods for the reconstruction of the projections of process models were implemented as a component in the composition of BPMN - the editor of workflow processes.

REFERENCES

1. Van der Aalst W.M.P. *Process Mining: Discovery, Conformance and Enhancement of Business Processes*. Berlin: Springer-Verlag, 2011. 352 p.

2. Barsegyan A.A., Kupriyanov M.S., Kholod I.I., Tess M.D., Elizarov S.I. *Analyz dannyh I processov* [Data mining and process mining]. St. Petersburg: BKhV-Peterburg, 2009. 512 p. (In Russian)

3. Romanchenko E.V. Osnovnye tendentsii razvitiya SED v Rossii [The main trends in the development of EDS in Russia]. Sovremennye tekhnologii deloproizvodstva i dokumentooborota [Modern technologies of records management and document management]. 2015. No. 8. URL: http://e.deloprost.ru/article.aspx?aid=419473 (date of access 05.10.2018). (In Russian)

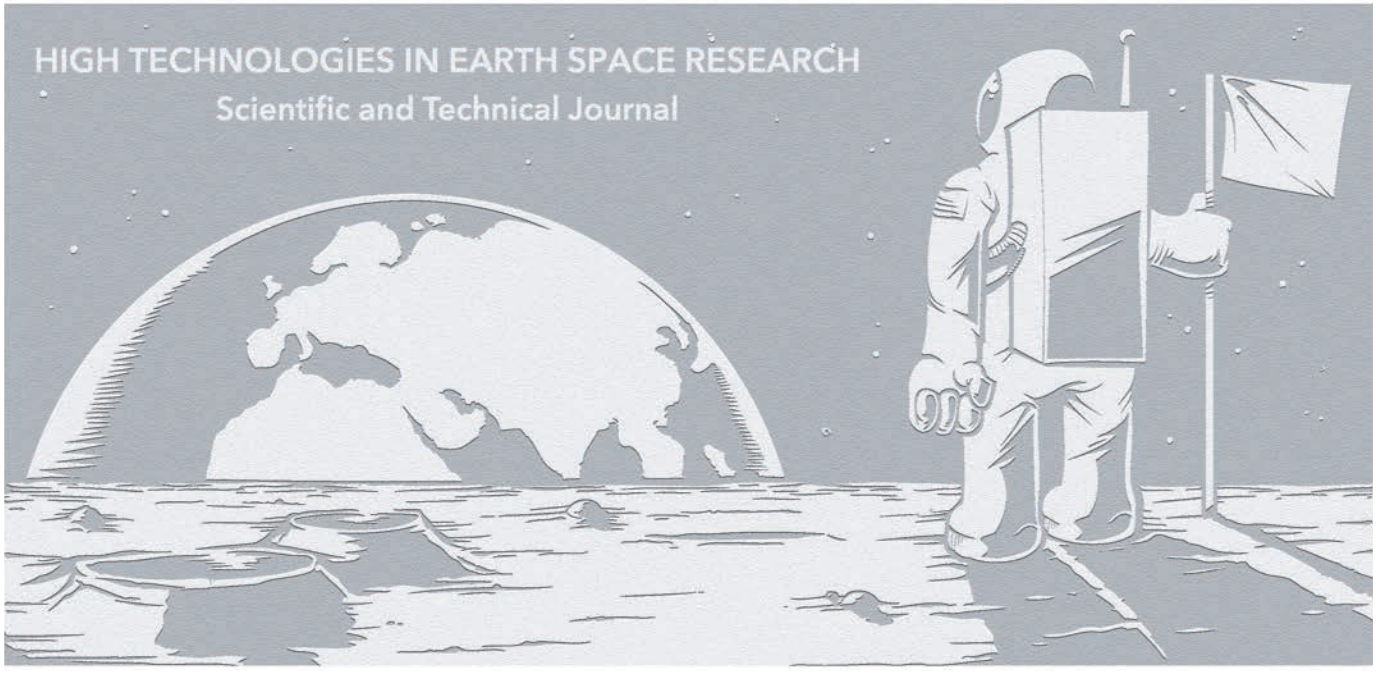
4. Mokryy V. Yu. *Sistemy elektronnogo dokumentooborota* [EDM system]. St. Petersburg: Info-da, 2018. 48 p. (In Russian)

5. Mikheev A.G. *Sistemy upravleniya biznes-protsessami i administrativnymi reglamentami na primere svobodnoy programmy RunaWFE* [Business process management systems and administrative regulations on the example of the free RunaWFE program]. Moscow: Al't Linuks, 2011. 178 p. (In Russian)

6. Van der Aalst W.M.P., Weijters A.J.M.M., Maruster L. Workflow Mining: Discovering process models from event logs. *IEEE Transactions on Knowledge & Data Engineering*. 2004. Vol. 16. No. 5. Pp. 1128–1142.
7. Van der Aalst W.M.P., van Dongen B.F. Discovering Workow Performance Models from Timed Logs. *EDCIS2002: Engineering and Deployment of Cooperative Information Systems*. LNCS. Berlin: Springer, 2002. Vol. 2480. Pp. 45–63.
8. Van der Aalst W.M.P., Weijters A.J.M.M. Process mining: a research agenda. *Computers in Industry*. 2004. No. 53(3). Pp. 231–244.
9. De Medeiros A.K. A, van Dongen B.F., van der Aalst W.M.P., Weijters A.J.M.M. *Process Mining: Extending the α-algorithm to Mine Short Loops*. Eindhoven University of Technology, Eindhoven, 2004. URL: https://pure.tue.nl/ws/files/1864325/576199.pdf.
10. Paklin N.B., Oreshkov V.I. *Biznes-analitika: ot dannykh k znaniyam* [Business intelligence: from data to knowledge]. St. Petersburg: Piter, 2009. 624 p. (In Russian)
11. Marmanis Kh., Babenko D. *Algoritmy intellektual'nogo interneta. Peredovye metodiki sbora, analiza i obrabotki dannykh* [Algorithms of the intelligent web. Advanced methods of data collection, analysis and processing]. St. Petersburg: Simvol-Plyus, 2011. 480 p.
12. Certificate of registration of a computer program RF 2017663083. Podsistema zashchishchennogo elektronnogo dokumentooborota "Tsera" [Subsystem protected electronic document "CERA"]. Vasil'ev N.V., Kompanets A.N., Sopin D.S.; applicant and owner of PJSC "Inteltekh" (EN). Dclared. 06.10.17. Publ. 24.11.17. Register of computer programs. 1 p. (In Russian)
13. Van Dongen B., de Medeiros A., Verbeek H., Weijters A., van der Aalst W.M.P. The prom framework: A new era in process mining tool support. *ICATPN2005: Applications and Theory of Petri Nets*. LNCS. Springer, 2005. Vol. 3536. Pp. 444–454.
14. Van Dongen B.F., van der Aalst W.M.P. EMiT: A Process Mining Tool. *ICATPN2004: Applications and Theory of Petri Nets*. LNCS. Springer, 2004. Vol. 3099. Pp. 454–463.
15. Leemans S.J.J., Fahland D., van der Aalst W.M.P. Discovering Block-Structured Process Models from Event Logs – A Constructive Approach. *Petri Nets*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013. Vol. 7927. Pp. 311–329.

INFORMATION ABOUT AUTHORS:
Vasiliev N.V., PhD, Head division of department Joint-Stock Company "Inteltech";
Zabrodin O.V., Engineer of the Joint-Stock Company "Inteltech";
Kulikov D.V., Engineer of the Joint-Stock Company "Inteltech".

For citation: Vasiliev N.V., Zabrodin O.V., Kulikov D.V. Process Mining methods in the secure electronic document content record management systems. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 38–50. doi: 10.24411/2409-5419-2018-10186 (In Russian)



doi: 10.24411/2409-5419-2018-10187

АНАЛИЗ ИЕРАРХИЧЕСКОЙ МОДЕЛИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПАРАМЕТРАМИ РАДИОЛИНИЙ КОГНИТИВНОЙ РАДИОСИСТЕМЫ

БЛАГОДАТСКИЙ
Григорий Александрович[1]

КОПЫСОВ
Андрей Николаевич[2]

ХВОРЕНКОВ
Владимир Викторович[3]

БАТУРИН
Иван Сергеевич[4]

АННОТАЦИЯ

Рассмотренная в работе иерархическая модель описывает радиосистему, предназначенную для работы в труднодоступных районах страны, не имеющих какой-либо инфраструктуры. Применение коротковолновой радиолинии требует особого внимания, так как передача информации в таких радиолиниях сопрягается с преодолением ряда факторов: погодных условий, времени суток, помеховой обстановке. В работе рассмотрена пятиуровневая модель когнитивной системы радиосвязи, представлено влияние сил (уровень I_1), акторов системы (уровень I_2), целей акторов (уровень I_3), параметров акторов (уровень I_4), воздействующих на процесс передачи сигналов на цель системы (уровень I_0). В результате исследования выявлено: установлено что значение влияния природных факторов и воздействий противника сравнимо, но в несколько раз меньше чем состояние системы радиосвязи; важное значение для эффективной передачи информации имеет устройство наблюдателя и регулятор и менее важное значение управляемый процесс и внутреннее состояние системы передачи информации; цель снижения количества ошибок при передаче информации и увеличение скорости передачи информации имеют важное значение для эффективной передачи информации, в сравнении со снижением вычислительной нагрузки на формирование сигнально-кодовых конструкций и снижением количества затрачиваемой энергии на передачу; наибольшую эффективность работы радиосистемы можно достигнуть за счет применения оптимальных алгоритмов обработки сигналов, и высокой мощности передаваемого сигнала; показано, что повышение скорости передачи информации без необходимой энергетики радиолинии и алгоритмов обработки сигналов не дадут ощутимого эффекта при передаче информации в сложных условиях.

КЛЮЧЕВЫЕ СЛОВА: когнитивные радиосистемы; анализ иерархий; системный анализ; метод Т. Саати; автоматическое управление; метод анализа иерархий.

Сведения об авторах:

[1]к.т.н., доцент, доцент кафедры информационных систем Ижевского государственного технического университета имени М.Т. Калашникова, г. Ижевск, Россия, blagodatsky@gmail.com

[2]к.т.н., доцент, заведующий кафедрой радиотехники Ижевского государственного технического университета имени М.Т. Калашникова, г. Ижевск, Россия, kan_kan@istu.ru@gmail.com

[3]д.т.н., профессор, профессор кафедры радиотехники Ижевского государственного технического университета имени М.Т. Калашникова, г. Ижевск, Россия, hvv@istu.ru

[4]аспирант кафедры радиотехники Ижевского государственного технического университета имени М.Т. Калашникова, г. Ижевск, Россия, baturin965@mail.ru

Для цитирования: *Благодатский Г.А., Копысов А.Н., Хворенков В.В., Батурин И.С.* Анализ иерархической модели автоматизированной системы управления параметрами радиолиний когнитивной радиосистемы // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 51–67. doi: 10.24411/2409-5419-2018-10187

Введение

Согласно определению Международного союза электросвязи (МСЭ; ITU) система когнитивного радио [1] — это радиосистема, использующая технологию, позволяющую ей получать знания о своей среде эксплуатации и географической среде, об установившихся правилах и о своем внутреннем состоянии, динамически и автономно корректировать эксплуатационные параметры и протоколы согласно полученным знаниям для достижения заранее поставленных целей и обучаться на основе полученных результатов. Таким образом, радиостанции, входящие в такую систему должны содержать устройства анализа состояния, как самой радиостанции, так и внешней географической, ситуационной и помеховой обстановки.

Решение задач управления динамическими объектами включает формирование математической модели с последующим исследованием свойств этой модели и синтезом регулятора. Объектами управления в информационной системе являются приемники и передатчики информации. Причем может быть управление параметрами как отдельно передатчика, например, управление мощностью, так и одновременное управление приемником и передатчиком, например, при выборе наилучшего канала связи.

В цифровых системах решение аналогичной задачи отличается большой гибкостью и имеет множество вариантов [2]. Выбор структурных решений при проектировании цифровых систем в значительной степени определяется особенностями решаемой задачи. Одним из подходов для решения данной задачи выступает многоагентный подход [3]. Отдельный агент рассматривается как механизм, способный повлиять на достижение цели, принятие решения. Каждый из агентов решает свою задачу, но способен обмениваться информацией друг с другом. Для организации процесса декомпозиции задачи в многоагентных системах создается либо система распределенного решения проблемы, либо децентрализованный искусственный интеллект. Для оценки влияния агентов в системе когнитивного радио применим метод анализа иерархий Т. Саати [4–5]. На сегодняшний день существуют примеры успешного применения метода анализа иерархий в различных областях применения: управление проектами по разработке инженерных приложений [6–10], отдельный обзор применения метода с момента его создания в работе [11], разработке промышленных установок по многоступенчатой ступенчатой переработке материалов [12], анализе аккредитационынх показателей ВУЗов [13], оценке заявок на участие в конкурсах по разработке сложных систем [14], проведении ранжирования спортсменов высокой квалификации [15], повышении эффективности функционирования предприятий [16].

1. Представление когнитивной радиосистемы в виде иерархии

На систему когнитивной радио связи воздействуют силы, формируемые природно-географическими факторами, противником, создающим активную помеховую обстановку и процессами, происходящими в работающей электрической части сети приемо-передатчиков радиосигналов. Радиостанции, входящие в такую систему должны содержать устройства анализа состояния, как самой радиостанции, так и внешней географической, ситуационной и помеховой обстановки, динамической и автономной корректировки эксплуатационных параметров и протоколов согласно полученным знаниям для достижения заранее поставленных целей. В системе должен быть и механизм обучения на основе полученных результатов работы системы (рис. 1).

Будем рассматривать систему передачи радиосигналов, как иерархическую систему. Выделим в системе множество уровней $I = \{I_i\}, i = \overline{1,m}$. На каждом уровне иерархии наблюдаются сложные взаимодействия с вышестоящими уровнями иерархии. Для формализации процесса принятия решений о повышении эффективности работы когнитивной системы связи применим метод анализа иерархий Т. Саати.

Рассмотрим уровни системы *I*.

Вершина системы представлена уровнем I_0, показывающим как работает система когнитивной радиосвязи.

На первом уровне системы I_1 выделим силы (1),

$$W_{I_1} = \{W_{I_1 j}\}, j = \overline{1, n_{I_1}} \quad (1)$$

оказывающие влияние на качественный прием-передачу сигналов. Как уже отмечалось силами будут: силы, формируемые процессами, происходящими в работающей электрической части сети приемо-передатчиков $(W_{I_1 1})$, противником, создающим помеховую обстановку $(W_{I_1 2})$ и природно-географические факторы $(W_{I_1 3})$.

На втором уровне системы I_2 выделим активные элементы (акторы), которые направляют силы. Введем аналогично (2)

$$W_{I_2} = \{W_{I_2 j}\}, j = \overline{1, n_{I_2}}, \quad (2)$$

где $W_{I_2 1}$ — внутреннее состояние системы, $W_{I_2 2}$ — устройство наблюдателя (для общности рассуждений) — приемник цифровых сигналов (декодер или, в случае одновременного выполнения процедуры демодуляции и декодирования, модем), $W_{I_2 3}$ — регулятор вырабатывающий управляющие воздействия, поступающие на приемник, передатчик и модем, $W_{I_2 4}$ — управляемый процесс передачи сигналов (код управляющих воздействий записывается в информа-

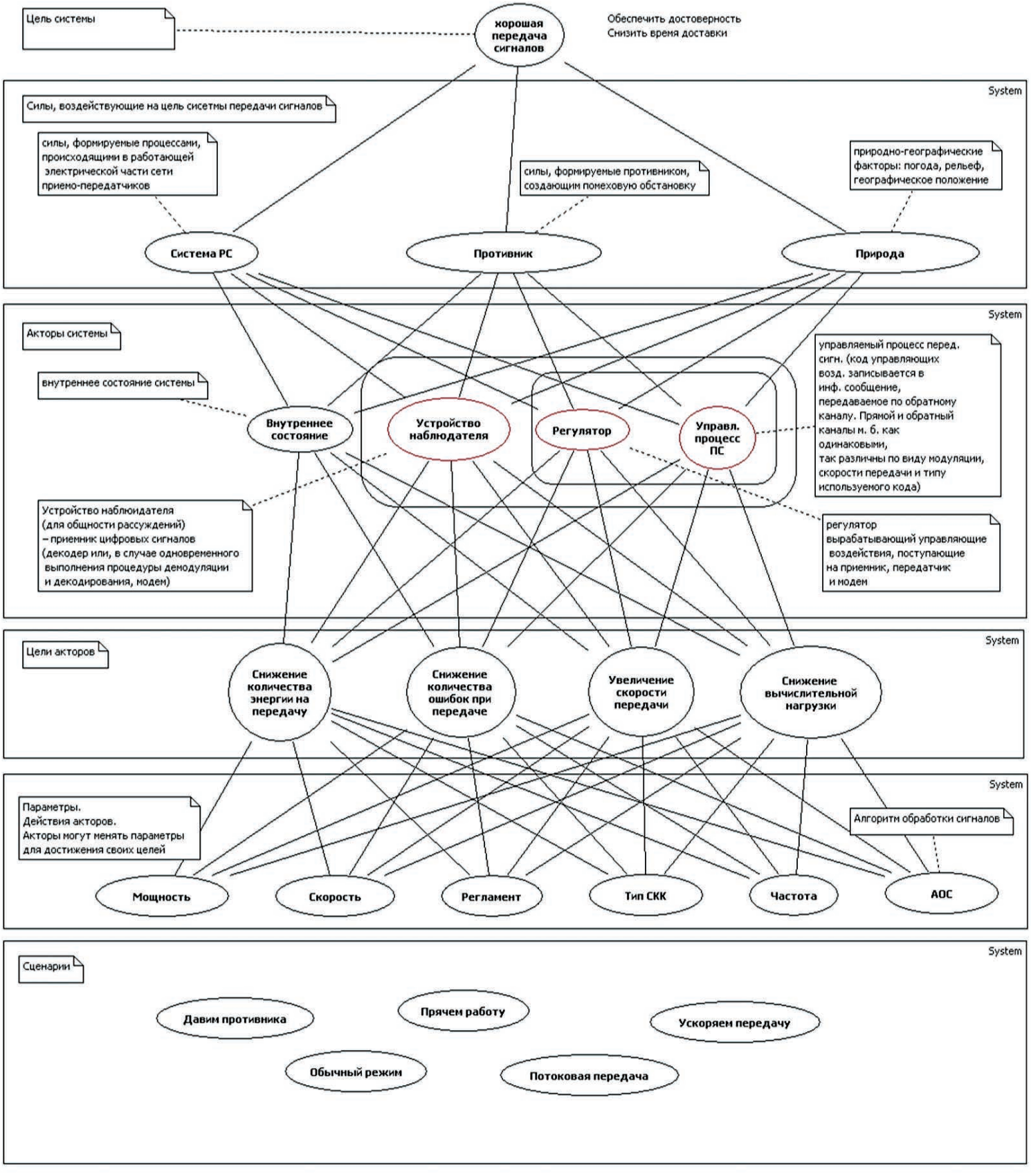


Рис. 1. Иерархическая модель когнитивной радиосистемы

ционное сообщение, передаваемое по обратному каналу. Прямой и обратный каналы могут быть как одинаковыми, так различны по виду модуляции, скорости передачи и типу используемого кода).

При проектировании такой системы требуется обеспечить выполнение противоречивых задач. Информацию надо передать с максимальной скоростью, принять с максимальной достоверностью и при этом затратить минимум энергетических и вычислительных ресурсов. Выделим уровень целей I_3 и его элементы (3)

$$W_{I_3} = \{W_{I_3 j}\}, j = \overline{1, n_{I_3}}, \quad (3)$$

где $W_{I_3 1}$ — максимизация скорости передачи данных, $W_{I_3 2}$ — максимизация достоверности передачи, $W_{I_3 3}$ — минимизация расхода энергии, $W_{I_3 4}$ — минимизация расхода вычислительных ресурсов.

Цели акторов могут быть достигнуты за счет возможных действий — уровень I_4. Выделим его элементы (4)

$$W_{I_4} = \{W_{I_4 j}\}, j = \overline{1, n_{I_4}}, \quad (4)$$

где $W_{I_4 1}$ — управление мощностью передатчика, $W_{I_4 2}$ — управление скоростью передачи, $W_{I_4 3}$ — управление несущей частотой, $W_{I_4 4}$ — управление регламентом связи, $W_{I_4 5}$ — управление типом принимаемых СКК, $W_{I_4 6}$ — управление алгоритмом обработки сигналов.

Возможные комбинации управляемых параметров формируют уровень сценариев I_5, состоящий из множества его элементов $W_{I_5} = \{W_{I_5 j}\}, j = \overline{1, n_{I_5}}$.

Наша цель установить влияние элементов находящихся на уровне I_4 на вершину иерархии.

2. Применение метода анализа иерархий Т. Саати к задаче выявления весов элементов

Установим влияние $I_1 \rightarrow I_0$ сил, расположенных на уровне I_1 на цель системы I_0. Для этого будем попарно сравнивать важность элементов $W_{I_1} = \{W_{I_1 j}\}, j = \overline{1, n_{I_1}}$ по шкале отношений [1,9], где доминирование элемента $W_{I_1 k}$ по отношению $W_{I_1 m}$ обозначается целым числом из шкалы отношений a_{km}. Проведя $C^2_{n_{I_1}}$ сравнений заполним ими матрицу $A_{I_1} = \left[a_{ij} \right]$ парных сравнений, размерности $n_{I_1} \times n_{I_1}$.

Для заполнения матрицы A_{I_1} необходимо ответить на вопрос какую значимость по отношению к эффективной работе системы когнитивной связи имеют элементы уровня I_1 взятые попарно. Уровень I_1 состоит из 3 элементов: «Система радиостанций» — силы, формируемые процессами, происходящими в работающей электрической части сети приемо-передатчиков ($W_{I_1 1}$), «Противник» — силы, формируемые противником, создающим помеховую обстановку ($W_{I_1 2}$) и «Природа» — природно-географические факторы ($W_{I_1 3}$). Приведем сравнения в табл. 1.

Заполним матрицу A_{I_1}, полагая по Саати, что сравнение влияния $W_{I_1 m}$ на I_0 по отношению к $W_{I_1 k}$ заменяется обратной величиной влияния влияния $W_{I_1 k}$ на I_0 по отношению к $W_{I_1 m}$ $a_{mk} = \frac{1}{a_{km}}$. Необходимо учитывать равную значимость влияния элемента в сравнении с самим собой $a_{kk} = 1$. Результат приведем в табл. 2.

Найдя правый собственный вектор ω'_{I_1} матрицы A_{I_1}, соответствующий максимальному собственному числу решая уравнение (5)

$$A_{I_1} \omega'_{I_1} = \lambda_{\max I_1} \omega'_{I_1}, \quad (5)$$

Рис. 2. Влияние $I_1 \rightarrow I_0$ сил, расположенных на уровне I_1 на цель системы I_0

Таблица 1

Влияние $I_1 \rightarrow I_0$ сил, расположенных на уровне I_1 на цель системы I_0

№	Сравнение	Результат	Объяснение
1	$W_{I_1 1}$ & $W_{I_1 2}$	a_{12}=7 очень сильное влияние	$W_{I_1 1}$ — корректная работа системы радиостанций оказывает значительно большее влияние на результат, в сравнении с $W_{I_1 2}$ — противодействием противника, т.к. в условиях гористой местности сложно осуществить широкополосную помеху для приема-передачи радиосигналов.
2	$W_{I_1 1}$ & $W_{I_1 3}$	a_{13}=5 сильное влияние	$W_{I_1 1}$ — корректная работа системы оказывает сильное влияние на результат, в сравнении с $W_{I_1 3}$ — природно-географическими факторами, т.к. технические устройства системы радиостанций предназначены для преодолении этих факторов.
3	$W_{I_1 2}$ & $W_{I_1 3}$	a_{23}=1 равное влияние факторов	Воздействие $W_{I_1 2}$ — природно-географических факторов (отсутствие прямой видимости: перепады высот до 4000 м, внезапные ливневые осадки, густая облачность, густая растительность в ущельях до 1800 м, трудность во взаимодействии с ионосферой — грозовые облака) в гористой местности оказывает равное воздействие на результат, в сравнении с действием $W_{I_1 3}$ — противника, которому трудно осуществить широкополосную помеху в труднодоступных районах.

Таблица 2

Парное сравнение влияния сил на цель системы («хорошая передача сигналов» — обеспечить достоверность, снизить время доставки)

A_{I_1}	$W_{I_1 1}$	$W_{I_1 2}$	$W_{I_1 3}$
$W_{I_1 1}$	1	$a_{12} = 7$	$a_{13} = 5$
$W_{I_1 2}$	$\frac{1}{a_{12}} = \frac{1}{7}$	1	$a_{23} = 1$
$W_{I_1 3}$	$\frac{1}{a_{13}} = \frac{1}{5}$	$\frac{1}{a_{23}} = 1$	1

Введем итеративную процедуру [17] нахождения собственного вектора, соответствующего максимальному собственному числу.

Пусть $y^{(0)}=\{1,\ldots,1\}$ единичный вектор размерности n_{I_1}. Запустим итеративный процесс $y^{(k)} = A_{I_1} y^{(k-1)} = A_{I_1}^{k-1} y^{(0)}$ до достижения (6)

$$\varepsilon^{(k)} = \left| \frac{y_j^{(k)}}{y_j^{(k-1)}} - \frac{y_j^{(k-1)}}{y_j^{(k-2)}} \right| \le \varepsilon, \qquad (6)$$

где ε — погрешность вычислений $\lambda_{\max I_1} = \frac{y_j^{(k)}}{y_j^{(k-1)}}$.

Получившийся на последнем шаге итерационного процесса вектор $y^{(k)}$ есть решение уравнения $A_{I_1} \omega'_{I_1} = \lambda_{\max I_1} \omega'_{I_1}$.

Проведя нормирование вектора ω'_{I_1}, по сумме координат получим вектор (7)

$$\omega_{I_1} = \left\{ \frac{\omega'_{I_1 i}}{\sum_{j=1}^{n_{I_1}} \omega'_{I_1 j}} \right\}, i = \overline{1, n_{I_1}}, \qquad (7)$$

где ω_{I_1} вектор весов влияния $I_1 \rightarrow I_0$ сил, расположенных на уровне I_1 на цель системы I_0.

В результате расчетов получим ω_{I_1}=(0,75; 0,12; 0,13). Данные веса свидетельствуют о том, что погодные факторы и противник вносят равный вклад в успешную работу системы (табл. 3). Суммарно вклад факторов противника и погоды дают 25% влияния на успешную работу.

Таблица 3

Влияние сил на цель системы

	I_0
Силы	ω_{I_1}
$W_{I_1 1}$ — силы, формируемые процессами, происходящими в работающей электрической части сети приемо-передатчиков	0,75
$W_{I_1 2}$ — противник, создающий помеховую обстановку	0,12
$W_{I_1 3}$ — природно-географические факторы	0,13

ОС = 0,05 <0,1

В качестве меры корректности суждений вводится отношение согласованности (ОС) — отношение индекса согласованности (ИС) матрицы парных сравнений A_{I_j} к случайному индексу (СИ) — ИС для квадратной матрицы размерности $n \times n$ заполненной случайными числами. Для матриц размерности $n \times n$ ИС рассчитывается по формуле $\text{ИС} = \frac{\lambda_{\max} - n}{n-1}$ ОС $\le 0{,}1$ считается допустимым для согласованности матрицы парных сравнений.

Проведя аналогичные вычисления, получим все векторы ω_{I_j}, $j = \overline{1,4}$ влияния элементов уровней $I_j \to I_{j-1}$ в иерархии I.

3. Формирование оценочных матриц

Будем рассматривать иерархию уровней по нисходящему процессу. Начнем с уровня I_2 (уровень активных элементов системы — «акторов», рис. 3)

$$I_1 (I_2 \to I_1)$$

Рассмотрим влияние его элементов на вышестоящий уровень I_1 (табл. 4). Уровень I_2: $W_{I_2 1}$ — внутреннее состояние системы, $W_{I_2 2}$ — устройство наблюдателя (для общности рассуждений) — приемник цифровых сигналов (декодер или, в случае одновременного выполнения процедуры демодуляции и декодирования, модем), $W_{I_2 3}$ —

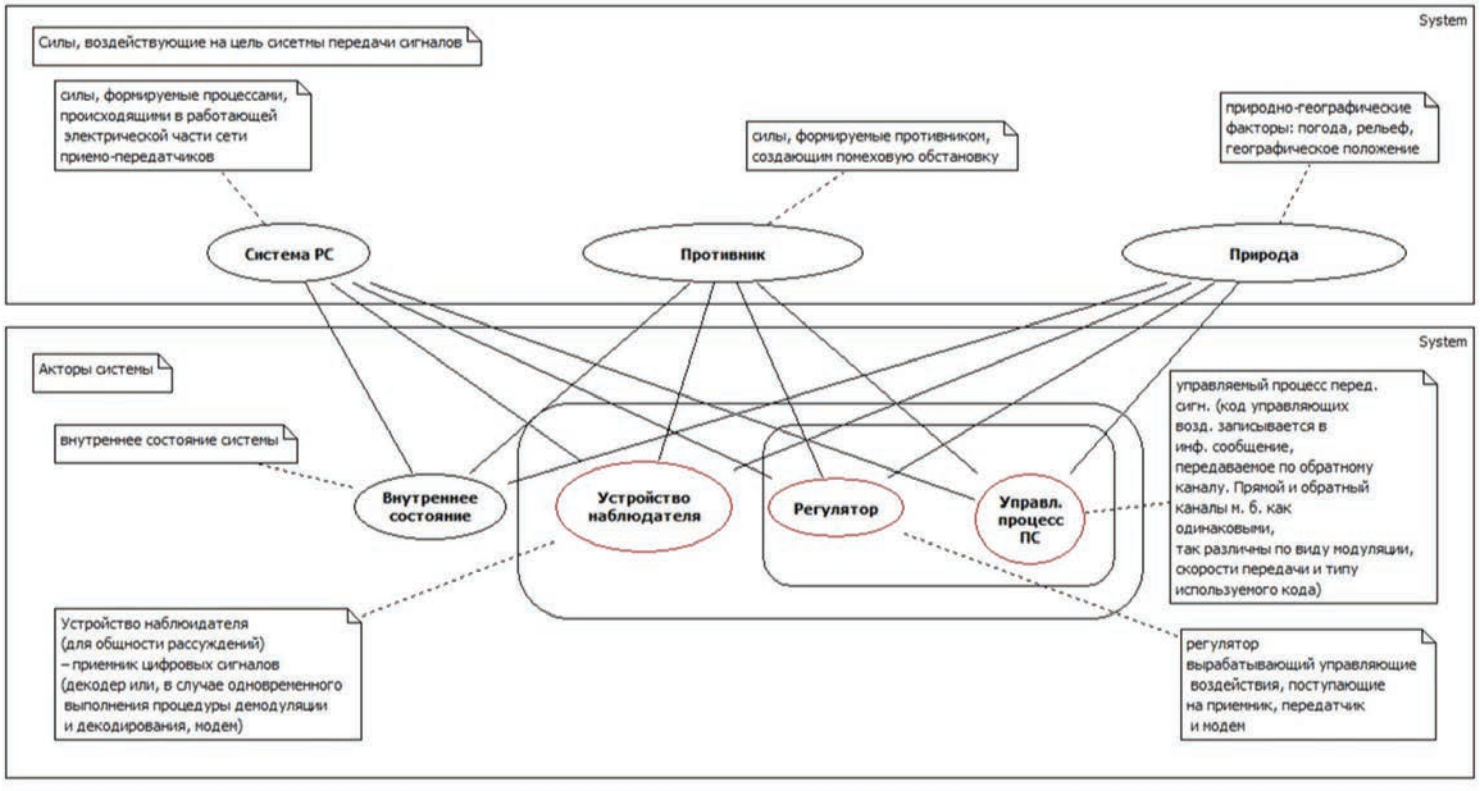


Рис. 3. Влияние акторов, расположенных на уровне I_2 на силы, расположенные на уровне

регулятор вырабатывающий управляющие воздействия, поступающие на приемник, передатчик и модем, $W_{I_2 4}$ — управляемый процесс передачи сигналов (код управляющих воздействий записывается в информационное сообщение, передаваемое по обратному каналу. Прямой и обратный каналы могут быть как одинаковыми, так различны по виду модуляции, скорости передачи и типу используемого кода).

Таблица 4

Влияние акторов на обеспечение $W_{I_1 1}$ — корректной работы системы радиостанций $I_2 \rightarrow I_{11}$

№	Сравнение	Результат	Объяснение
1	$W_{I_2 1}$ & $W_{I_2 2}$	5 сильное превосходство	$W_{I_2 1}$ — внутреннее состояние системы дает значительно больший вклад в корректную работу системы в сравнении с $W_{I_2 2}$ — устройством наблюдателя, т.к. стабильность внутреннего состояния оказывает большее влияние на успешную передачу информации, чем возможность изменение параметров радиосистемы
2	$W_{I_2 1}$ & $W_{I_2 3}$	3 некоторое превосходство	$W_{I_2 1}$ — внутреннее состояние системы дает больший вклад в корректную работу системы в сравнении с $W_{I_2 3}$ — регулятором, т.к. стабильность внутреннего состояния оказывает большее влияние на успешную передачу информации, чем возможность анализа текущего состояния и внесения изменений в работу системы
3	$W_{I_2 4}$ & $W_{I_2 2}$	3 некоторое превосходство	$W_{I_2 4}$ — управляемый процесс передачи сигналов дает больший вклад в корректную работу системы в сравнении с $W_{I_2 2}$ — устройством наблюдателя, т.к. возможность управления системой на основе информации, получаемой по обратной связи имеет большее значение, чем набор возможностей для ее адаптации
4	$W_{I_2 3}$ & $W_{I_2 2}$	3 некоторое превосходство	$W_{I_2 3}$ — регулятор дает больший вклад в корректную работу системы в сравнении с $W_{I_2 2}$ — устройством наблюдателя, т.к. устройство наблюдателя должно работать в совокупности с регулятором, но без него не имеет практического смысла
5	$W_{I_2 4}$ & $W_{I_2 2}$	3 некоторое превосходство	$W_{I_2 4}$ — управляемый процесс передачи сигналов дает больший вклад в корректную работу системы в сравнении с $W_{I_2 2}$ — устройством наблюдателя, т.к. возможность изменения параметров без получения информации по обратному каналу связи не имеет практического смысла
6	$W_{I_2 4}$ & $W_{I_2 3}$	3 некоторое превосходство	$W_{I_2 4}$ — управляемым процесс дает больший вклад в корректную работу системы передачи сигналов системы в сравнении с $W_{I_2 3}$ — регулятором т.к. возможность изменения параметров без получения информации по обратному каналу связи не имеет практического смысла

По данным табл. 4 построим матрицу парных сравнений (табл. 5).

Таблица 5

Матрица парных сравнений $A_{I_2 1}$ и нормированное значение вектора влияния акторов на обеспечение $W_{I_1 1}$ — корректной работы системы радиостанций $I_2 \rightarrow I_{11}$

Акторы I_2	$W_{I_2 1}$	$W_{I_2 2}$	$W_{I_2 3}$	$W_{I_2 4}$	$\omega_{I_{21}}$
$W_{I_2 1}$	1	5	3	1	0,40
$W_{I_2 2}$	0,2	1	1/3	1/3	0,08
$W_{I_2 3}$	1/3	3	1	1/3	0,16
$W_{I_2 4}$	1	3	3	1	0,36

ОС ≈ 0,07 < 0,1

Оставшиеся матрицы уровня I_2 формируются аналогично (табл. 6–7). Матрицы описывают влияние акторов на противодействие природным факторам и преднамеренным помехам.

Таблица 6

Матрица парных сравнений $A_{I_2 2}$ и нормированное значение вектора влияния акторов на преодоление $W_{I_1 2}$ — противодействия противника $I_2 \rightarrow I_{12}$

Акторы I_2	$W_{I_2 1}$	$W_{I_2 2}$	$W_{I_2 3}$	$W_{I_2 4}$	$\omega_{I_{22}}$
$W_{I_2 1}$	1	0,5	1/3	3	0,16
$W_{I_2 2}$	2	1	1	7	0,37
$W_{I_2 3}$	3	1	1	7	0,41
$W_{I_2 4}$	1/3	1/7	1/7	1	0,05

ОС ≈ 0,04 < 0,1

Таблица 7

Матрица парных сравнений $A_{I_2 3}$ и нормированное значение вектора влияния акторов на преодоление $W_{I_1 3}$ — природно-географической обстановки $I_2 \rightarrow I_{13}$

Акторы I_2	$W_{I_2 1}$	$W_{I_2 2}$	$W_{I_2 3}$	$W_{I_2 4}$	$\omega_{I_{23}}$
$W_{I_2 1}$	1	0,5	1/3	3	0,17
$W_{I_2 2}$	2	1	3	3	0,44
$W_{I_2 3}$	3	1/3	1	5	0,31
$W_{I_2 4}$	1/3	1/3	0,2	1	0,08

ОС ≈ 0,14 < 0,1. Отношение согласованности больше порогового — требуется уточнение суждений.

Запишем векторы приоритетов $\omega_{I_2 i}, i = \overline{1,..|I_1|}$ для оценочных матриц $A_{I_2 i}, i = \overline{1,..|I_1|}$ уровня I_2 в виде матрицы $W_{I_2} = \{\omega_{I_2 i}\}, i = \overline{1,..|I_1|}$, где $|I_1|$ — мощность множества элементов уровня I_1 (табл. 8).

Таблица 8

Матрица $W_{I_2} = \{\omega_{I_2 i}\}, i = \overline{1,..|I_1|}$ влияния акторов системы на силы, оказывающие влияние на качественный прием-передачу сигналов

Силы I_1	$W_{I_1 1}$ — «Система радиостанций»	$W_{I_1 2}$ — «Противник»	$W_{I_1 3}$ — «Природа»
Акторы I_2	$\omega_{I_{21}}$	$\omega_{I_{22}}$	$\omega_{I_{23}}$
$W_{I_2 1}$ — внутреннее состояние системы	0,40	0,16	0,17
$W_{I_2 2}$ — устройство наблюдателя	0,08	0,37	0,44
$W_{I_2 3}$ — регулятор, вырабатывающий управляющие воздействия	0,16	0,41	0,31
$W_{I_2 4}$ — управляемый процесс передачи сигналов	0,36	0,05	0,08

Перейдем к уровню I_3 (уровень целей, рис. 4):

$W_{I_3 1}$ — максимизация скорости передачи данных,

$W_{I_3 2}$ — максимизация достоверности передачи (снижение числа ошибок),

$W_{I_3 3}$ — минимизация расхода энергии,

$W_{I_3 4}$ — минимизация расхода вычислительных ресурсов.

Рассмотрим его влияние на элементы уровня I_2.

Матрицы парных сравнений формируем аналогично предыдущему уровню (получим в результате табл. 9–12).

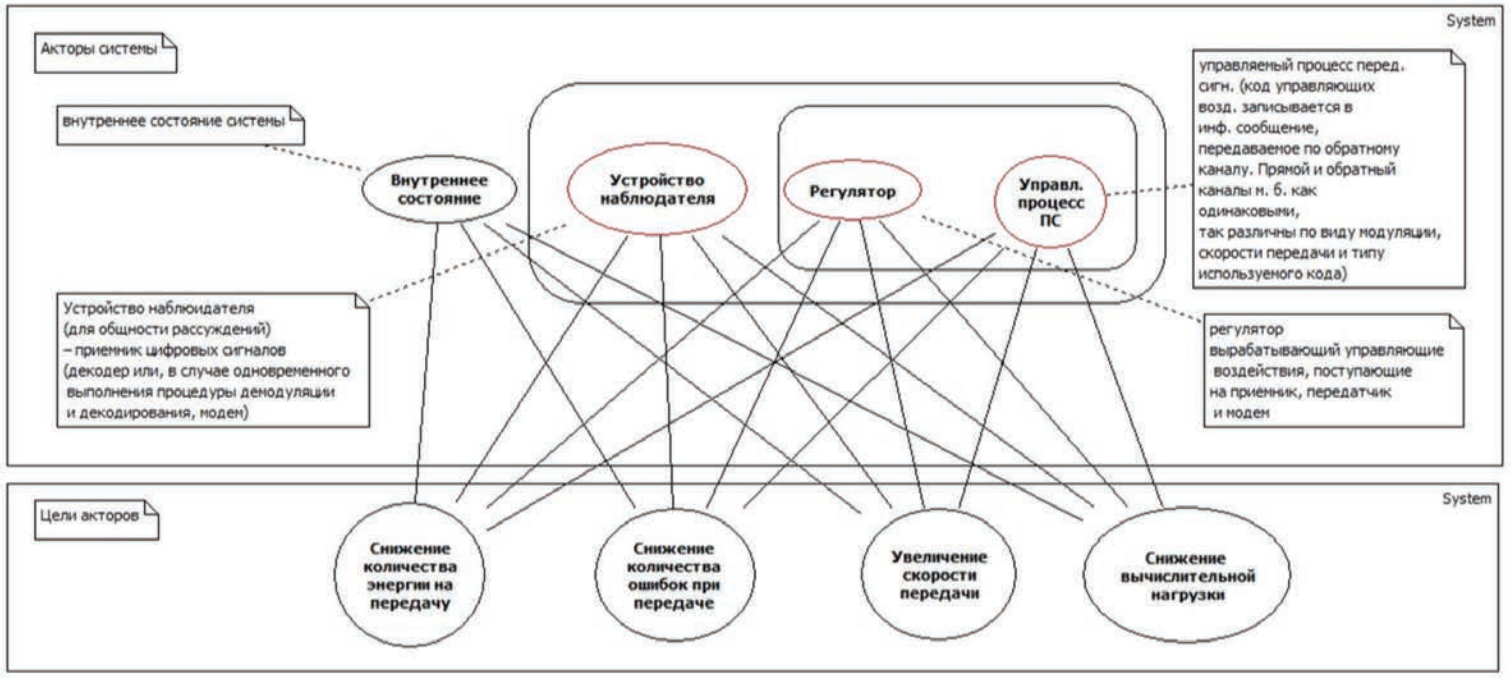


Рис. 4. Влияние $I_3 \rightarrow I_2$ целей акторов расположенных на уровне I_3 на акторы, расположенные на уровне I_2.

Таблица 9

Матрица парных сравнений $A_{I_3 1}$ и нормированное значение вектора влияния целей акторов на $W_{I_2 1}$ — внутреннее состояние $I_3 \rightarrow I_{21}$

Цели I_3	$W_{I_3 1}$	$W_{I_3 2}$	$W_{I_3 3}$	$W_{I_3 4}$	$\omega_{I_{31}}$
$W_{I_3 1}$	1	7	5	1	0,43
$W_{I_3 2}$	1/7	1	1/3	1	0,11
$W_{I_3 3}$	0,2	3	1	1/7	0,12
$W_{I_3 4}$	1	1	7	1	0,34

ОС = 0,07 < 0,1

Таблица 10

Матрица парных сравнений $A_{I_3 2}$ и нормированное значение вектора влияния целей акторов на $W_{I_2 2}$ — устройство наблюдения $I_3 \rightarrow I_{22}$

Цели I_3	$W_{I_3 1}$	$W_{I_3 2}$	$W_{I_3 3}$	$W_{I_3 4}$	$\omega_{I_{32}}$
$W_{I_3 1}$	1	1/7	1/7	7	0,12
$W_{I_3 2}$	7	1	1	7	0,43
$W_{I_3 3}$	7	1	1	5	0,41
$W_{I_3 4}$	1/7	1/7	0,2	1	0,04

ОС = 0,03 < 0,1

Таблица 11

Матрица парных сравнений $A_{I_3 3}$ и нормированное значение вектора влияния целей акторов на $W_{I_2 3}$ — регулятор $I_3 \rightarrow I_{23}$

Цели I_3	$W_{I_3 1}$	$W_{I_3 2}$	$W_{I_3 3}$	$W_{I_3 4}$	$\omega_{I_{33}}$
$W_{I_3 1}$	1	1/7	1/7	1	0,05
$W_{I_3 2}$	7	1	5	7	0,63
$W_{I_3 3}$	7	0,2	1	7	0,27
$W_{I_3 4}$	1	1/7	1/7	1	0,05

ОС = 0,1 ≤ 0,1

Таблица 12

Матрица парных сравнений $A_{I_3 4}$ и нормированное значение вектора влияния целей акторов на $W_{I_2 4}$ — управляемый процесс $I_3 \rightarrow I_{24}$

Цели I_3	$W_{I_3 1}$	$W_{I_3 2}$	$W_{I_3 3}$	$W_{I_3 4}$	$\omega_{I_{34}}$
$W_{I_3 1}$	1	0,2	0,2	5	0,11
$W_{I_3 2}$	5	1	5	7	0,59
$W_{I_3 3}$	5	0,2	1	7	0,26
$W_{I_3 4}$	0,2	1/7	1/7	1	0,04

ОС = 0,14 > 0,1. Отношение согласованности больше порогового, необходим пересмотр суждений.

Запишем векторы приоритетов $\omega_{I_3 i}, i = \overline{1,..|I_2|}$ для оценочных матриц $A_{I_3 i}, i = \overline{1,..|I_2|}$ уровня I_3 в виде матрицы $W_{I_3} = \{\omega_{I_3 i}\}, i = \overline{1,..|I_2|}$, где $|I_2|$ — мощность множества элементов уровня I_2 (табл. 13).

Таблица 13

Матрица $W_{I_3} = \{\omega_{I_3 i}\}, i = \overline{1,..|I_2|}$ влияния целей акторов на акторы системы

Акторы I_2	$W_{I_2 1}$ — внутреннее состояние системы	$W_{I_2 2}$ — устройство наблюдателя	$W_{I_2 3}$ — регулятор вырабатывающий управляющие воздействия	$W_{I_2 4}$ — управляемый процесс передачи сигналов
Цели акторов I_3	$\omega_{I_{31}}$	$\omega_{I_{32}}$	$\omega_{I_{33}}$	$\omega_{I_{34}}$
$W_{I_3 1}$ — максимизация скорости передачи данных	0,43	0,12	0,05	0,11
$W_{I_3 2}$ — максимизация достоверности передачи (снижение числа ошибок)	0,11	0,43	0,63	0,59
$W_{I_3 3}$ — минимизация расхода энергии	0,12	0,41	0,27	0,26
$W_{I_3 4}$ — минимизация расхода вычислительных ресурсов	0,34	0,04	0,05	0,04

Рассмотрим влияние уровня I_4 (действий акторов, рис. 5):

$W_{I_4 1}$ — управление мощностью передатчика,
$W_{I_4 2}$ — управление скоростью передачи,
$W_{I_4 3}$ — управление регламентом связи,
$W_{I_4 4}$ — управление типом принимаемых СКК,
$W_{I_4 5}$ — управление алгоритмом обработки сигналов.

Матрицы парных сравнений уровня и формирование нормированного вектора влияния элементов на вышестоящий уровень проведем по схеме, описанной выше (табл. 14).

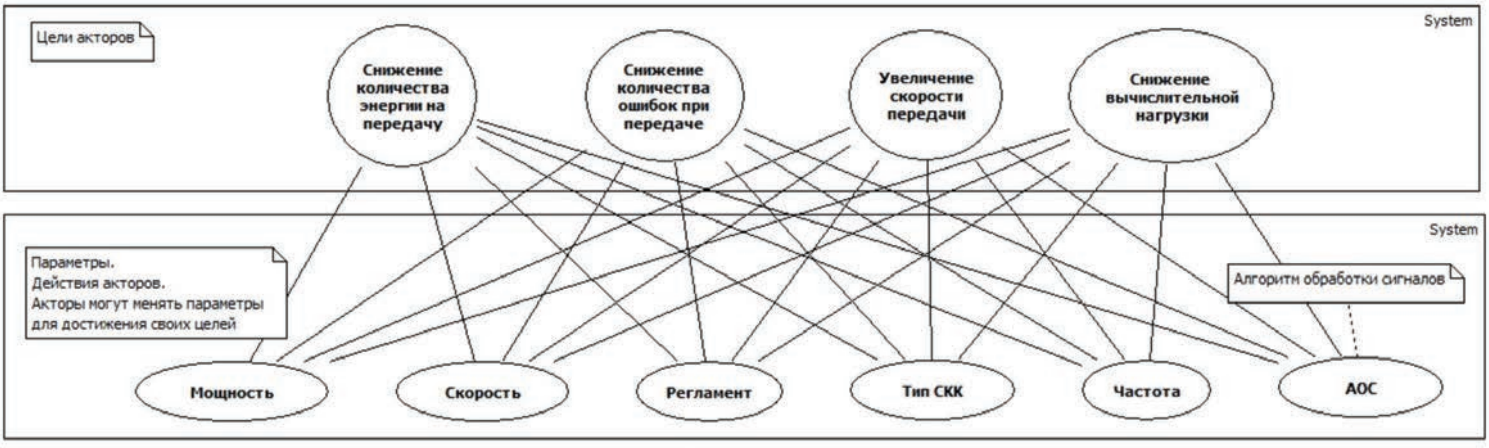


Рис. 5. Влияние $I_4 \rightarrow I_3$ действий акторов расположенных на уровне I_4 на цели акторов, расположенные на уровне I_3

Таблица 14

Матрица $W_{I_4} = \{\omega_{I_4 i}\}, i = \overline{1,..|I_3|}$ влияния действий акторов на цели акторов

Цели I_3	$W_{I_3 1}$ — максимизация скорости передачи данных	$W_{I_3 2}$ — максимизация достоверности передачи (снижение числа ошибок)	$W_{I_3 3}$ — минимизация расхода энергии	$W_{I_3 4}$ — минимизация расхода вычислительных ресурсов
Действия I_4	$\omega_{I_{41}}$	$\omega_{I_{42}}$	$\omega_{I_{43}}$	$\omega_{I_{44}}$
$W_{I_4 1}$ — управление мощностью передатчика	0,47	0,10	0,04	0,07
$W_{I_4 2}$ — управление скоростью передачи	0,09	0,12	0,06	0,24
$W_{I_4 3}$ — управление регламентом связи	0,33	0,09	0,22	0,15
$W_{I_4 4}$ — управление типом принимаемых СКК	0,04	0,37	0,26	0,05
$W_{I_4 5}$ — управление алгоритмом обработки сигналов.	0,07	0,10	0,42	0,49

Таким образом, влияние элементов нижнего уровня иерархии можно вычислить, как

$$\omega_{I_4} = W_{I_4}\omega_{I_3} = W_{I_4}W_{I_3}\omega_{I_2} = W_{I_4}W_{I_3}W_{I_2}\omega_{I_1}$$

4. Результаты расчетов

Результаты расчетов приведены в табл. 15–18 и на рис. 6–9.

Таблица 15

Влияние $I_1 \rightarrow I_0$

Влияние $I_1 \rightarrow I_0$	ω_{I_1}
$W_{I_1 1}$ — силы, формируемые процессами, происходящими в работающей электрической части сети приемо-передатчиков	0,75
$W_{I_1 2}$ — противник, создающий помеховую обстановку	0,12
$W_{I_1 3}$ — природно-географические факторы	0,13

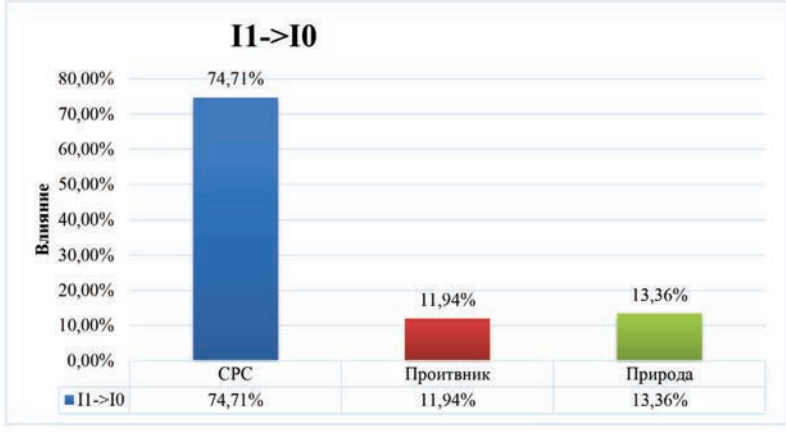


Рис. 6. Влияние уровня $I_1 \rightarrow I_0$

Таблица 16

Влияние $I_2 \rightarrow I_0$

	I_1			Влияние $I_2 \rightarrow I_0$ ω_{I_2}
Влияние $I_1 \rightarrow I_0$ ω_{I_1}	$W_{I_1 1}$	$W_{I_1 2}$	$W_{I_1 3}$	
	74,71%	11,94%	13,36%	
$W_{I_2 1}$ — внутреннее состояние системы	12,47%	4,77%	2,16%	19,40%
$W_{I_2 2}$ — устройство наблюдателя	33,19%	0,97%	4,96%	39,12%
$W_{I_2 3}$ — регулятор, вырабатывающий управляющие воздействия	23,16%	1,90%	5,50%	30,56%
$W_{I_2 4}$ — управляемый процесс передачи сигналов	5,89%	4,30%	0,73%	10,92%

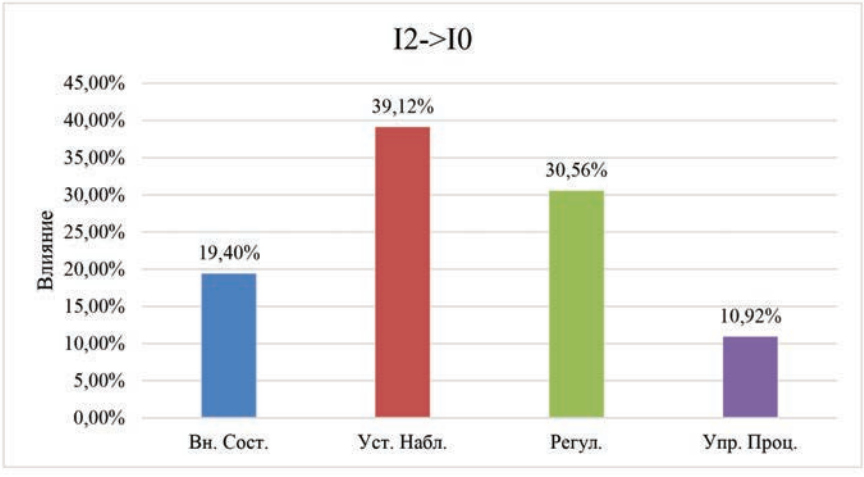


Рис. 7. Влияние $I_2 \rightarrow I_0$

Таблица 17

Влияние $I_3 \rightarrow I_0$

	I_2				Влияние $I_3 \rightarrow I_0$ ω_{I_3}
Влияние $I_2 \rightarrow I_0$ ω_{I_2}	$W_{I_2 1}$	$W_{I_2 2}$	$W_{I_2 3}$	$W_{I_2 4}$	
	19,40%	39,12%	30,56%	10,92%	
$W_{I_3 1}$ — максимизация скорости передачи данных	8,32%	4,67%	1,66%	1,15%	15,80%
$W_{I_3 2}$ — максимизация достоверности передачи (снижение числа ошибок)	2,13%	16,75%	19,11%	6,47%	44,45%
$W_{I_3 3}$ — минимизация расхода энергии	2,28%	15,99%	8,13%	2,86%	29,26%
$W_{I_3 4}$ — минимизация расхода вычислительных ресурсов	6,68%	1,71%	1,66%	0,44%	10,49%

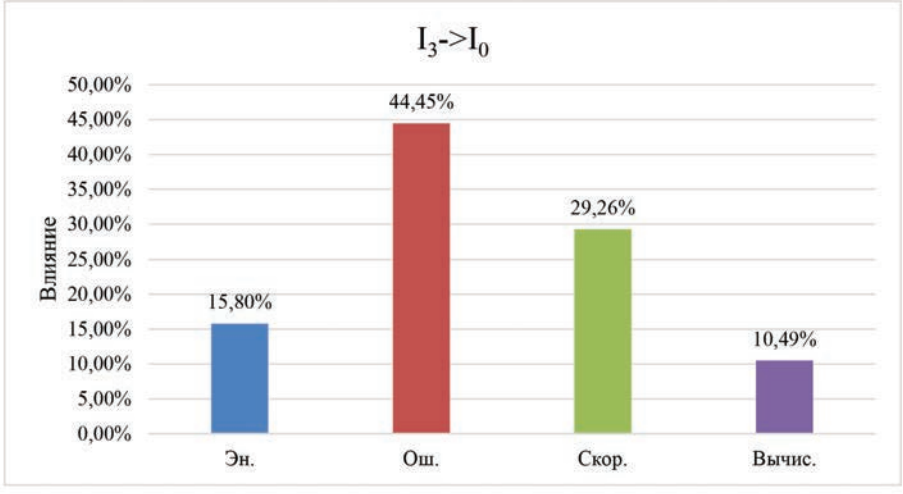


Рис. 8. Влияние $I_3 \rightarrow I_0$

Таблица 18

Влияние $I_4 \rightarrow I_0$

Влияние $I_3 \rightarrow I_0$ ω_{I_3}	I_3				Влияние $I_4 \rightarrow I_0$ ω_{I_4}
	$W_{I_3 1}$	$W_{I_3 2}$	$W_{I_3 3}$	$W_{I_3 4}$	
	15,80%	44,45%	29,26%	10,49%	
$W_{I_4 1}$ — управление мощностью передатчика	0,71%	14,47%	13,77%	0,72%	29,67%
$W_{I_4 2}$ — управление скоростью передачи	0,94%	4,31%	2,68%	2,49%	10,41%
$W_{I_4 3}$ — управление регламентом связи	3,42%	5,45%	9,62%	1,57%	20,06%
$W_{I_4 4}$ — управление типом принимаемых СКК	4,11%	3,80%	1,15%	0,57%	9,63%
$W_{I_4 5}$ — управление алгоритмом обработки сигналов	6,62%	16,43%	2,04%	5,15%	30,23%

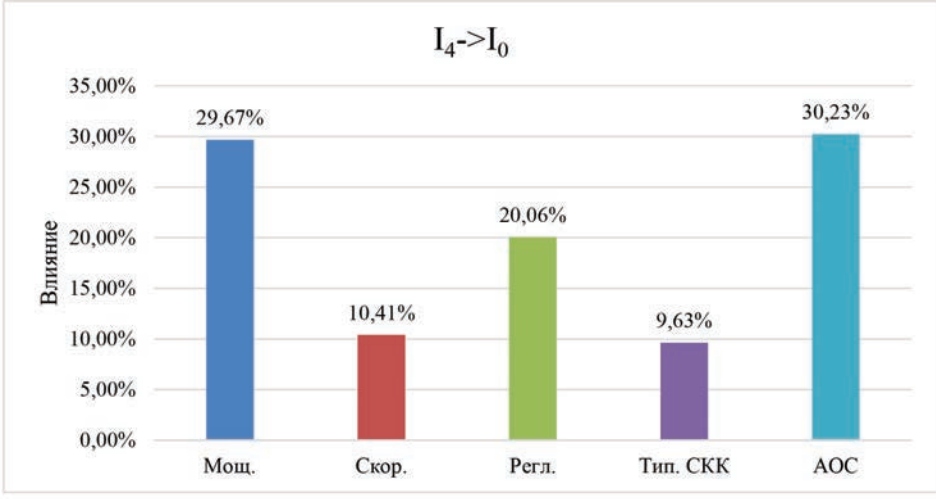


Рис. 9. Влияние $I_4 \rightarrow I_0$ — влияние параметров приемопередающих средств радиосистемы на эффективную передачу сигналов.

Основные выводы по работе

Рассмотрим и интерпретируем основные результаты моделирования когнитивной радиосистемы. Для этого рассмотрим влияние каждого уровня цель системы — эффективную передачу сигнала.

Рассмотрим влияние уровня I_1. На рис. 6. представлено влияние сил, воздействующих на цель передачи сигналов (уровень I_0) на цель системы (уровень I_1) по данным табл 16. Из представленной диаграммы видно, что значение влияния природных факторов и воздействий противника сравнимо, но в несколько раз меньше чем состояние системы радиосвязи. Это говорит о том, что корректно работающая радиосистема способна противостоять воздействующим дестабилизирующим факторам природного характера и преднамеренных помех.

На рис. 7 представлено влияние акторов системы (уровень I_2) на цель системы (уровень I_0) по данным табл. 17. Из представленной диаграммы видно, что важное значение для эффективной передачи информации имеет устройство наблюдателя и регулятор и менее важное значение управляемый процесс и внутреннее состояние системы передачи информации. Это связано с тем, что устройство наблюдателя включает в себя основные параметры приемных трактов радиосредств системы. При работе радиосистемы, это очень важно, т.к. радиообмен начинается всегда на начальных параметрах радиосистемы, а ее работа в этот момент

зависит от возможностей обнаружения и декодирования сигнала на начальных установках и восприятия регулирующего воздействия. В дальнейшем по результатам оценки канала связи и формирования управляющих процессов на внутреннее состояние радиосистемы происходит корректировка параметров для улучшения передачи информации.

На рис. 8 представлено влияние целей акторов системы (уровень I_3) на цель системы (уровень I_0) по данным табл. 18. Из представленной диаграммы видно, цель снижения количества ошибок при передаче информации и увеличение скорости передачи информации имеют важное значение для эффективной передачи информации, в снижении со снижением вычислительной нагрузки и снижением количества затрачиваемой энергии на передачу. Это справедливо, т.к. основной задачей системы радиосвязи является передача информации, а не экономия вычислительных и энергетических ресурсов. Кроме того, параметры повышения скорости обмена и снижения количества ошибок находятся в обратном отношении с экономией ресурсов системы.

На рис. 9 представлено влияние параметров радиосистемы (уровень I_4) на цель системы (уровень I_0) по данным табл. 18. Из представленной диаграммы видно, что наибольшую эффективность работы радиосистемы можно достигнуть за счет применения оптимальных алгоритмов обработки сигналов, и высокой мощности передаваемого сигнала. Повышение скорости передачи информации без необходимой энергетики радиолинии и алгоритмов обработки сигналов не дадут ощутимого эффекта при передаче информации в сложных условиях.

Литература

1. Definition of cognitive radio system. Report ITU-R SM.2152 09/2009. Electronic Publication, Geneva. 2009. С. 2. URL: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2152–2009-PDF-E.pdf (дата обращения 09.10.2018).

2. *Мирошник И.В., Никифоров В.О., Фрадков А.Л.* Нелинейное и адаптивное управление сложными системами. СПб.: Наука. 2000. 549 с.

3. *Городецкий В.И.* Многоагентные системы: современное состояние исследований и перспективы // Новости искусственного интеллекта. 1996. № 1. С. 44–59.

4. *Saaty T.L.* The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation (Decision Making Series). New York: McGraw-Hill. 1980. 287 p.

5. *Saaty R.W.* The Analityc Hierarchy Process — What it is and How it is Used // Mathematical Modelling. 1987. Vol. 9(3–5). Pp. 161–176.

6. *Quyen N.L.H.T.T., Nguyen P.T., Huynh V.D. B.* A hybrid multi criteria decision analysis for engineering project manager evaluation // International Journal of Advanced and Applied Sciences. 2017. Vol. 4. No. 4. Pp. 49–52.

7. *Lambert J.M.* The Extended Analytic Hierarchy Decision Method // Mathematical and Computer Modelling. 1991. Vol. 15 (11). Pp. 141–151.

8. *Ho W., Ma X.* The State-of-the-art Integrations and Applications of the Analytic Hierarchy Process // European Journal of Operational Research. 2017. Vol. 267(2). Pp. 399–414. URL: https://doi.org/10.1016/j.ejor.2017.09.007 (дата обращения 10.10.2018).

9. *Ivanco M., Hou G., Michaeli J.* Sensitivity Analysis Method to Address User Disparities in the Analytic Hierarchy Process // Expert Systems with Applications. 2017. Vol. 90. Pp. 111–126.

10. Aguilar-Lasserre A. A., Bautista Bautista M.A., Ponsich A., González Huerta M.A. An AHP-based decision-making tool for the solution of multiproduct batch plant design problem under imprecise demand // Computers & Operations Research. 2009. Vol. 36. Issue 3. Pp. 711–736. ISSN0305–0548. URL: https://doi.org/10.1016/j.cor.2007.10.029 (дата обращения 10.10.2018).

11. *Ishizaka A., Labib A.* Review of the main developments in the analytic hierarchy process // Expert Systems with Applications. 2011. No. 38. Pp. 14336–14345. URL: http://dx.doi.org/10.1016/j.eswa.2011.04.143 (дата обращения 10.10.2018).

12. *Жиров Д.К.* АСУ процессом механо-активации многокомпонентных материалов и ее системный анализ по критерию качества конечного продукта // Вестник Ижевского государственного технического университета. 2011. № 4 (52). С. 132–135.

13. *Благодатский Г.А.* Создание математической модели анализа структуры аккредитационных показателей ВУЗа с применением метода анализа иерархий // Вестник Ижевского государственного технического университета. 2010. № 2 (46). С. 115–118.

14. *Переведенцев Д.И.* Моделирование системы нечеткого логического вывода оценки наукоемких проектов // Автоматизация процессов управления. 2017. № 2 (48). С. 82–89.

15. *Горохов М.М.* Программно–инструментальное средство оценки тренированности спортсменов высших квалификаций // Вестник Ижевского государственного технического университета. 2016. № 2(70). С. 87–90.

16. *Благодатский Г.А.* Программно-инструментальные средства повышения эффективности внутренних бизнес-процессов предприятий. Ижевск: Изд-во ИжГТУ имени М.Т. Калашникова. 2015. 188 с.

17. *Калиткин Н.Н.* Численные методы. М.: Наука, 1978. С. 190–191.

ANALYSIS OF THE HIERARCHICAL MODEL OF THE AUTOMATED CONTROL SYSTEM OF THE PARAMETERS OF THE RADIO LINES OF THE COGNITIVE RADIO SYSTEM

GREGORY A. BLAGODATSKY,
Izhevsk, Russia, blagodatsky@gmail.com

VLADIVIR V. KHVORENKOV,
Izhevsk, Russia, blagodatsky@gmail.com

IVAN S. BATURIN,
Izhevsk, Russia, blagodatsky@gmail.com

KEYWORDS: cognitive radio systems; hierarchy analysis, system analysis; T. Saati method; automatic control; analytic hierarchy process.

ABSTRACT

The radio system hierarchical model designed to work in hard-to-reach areas of the country that do not have any infrastructure is described. The use of a short-wave radio link requires special attention, since the transmission of information in such radio links is coupled with overcoming a number of factors: weather conditions, time of day, interfering conditions. The paper considers a five-level model of a cognitive radio communication system, presents the influence of forces (level I1), actors of the system (level I2), targets of actors (level I3), parameters of actors (level I4) affecting the transmission of signals on the system target (level I0). As a result of the research, it was revealed that: it was established that the value of the influence of natural factors and the effects of the enemy is comparable, but several times less than the state of the radio communication system; the observer's device and the regulator are important for the effective transmission of information and the controlled process and the internal state of the information transmission system are less important; the goal of reducing the number of errors in the transmission of information and increasing the speed of information transmission are important for the effective transmission of information, in comparison with a reduction in the computational load on the formation of signal-code structures and a decrease in the amount of energy used for transmission; the highest efficiency of the radio system can be achieved through the use of optimal signal processing algorithms, and high power of the transmitted signal; it is shown that increasing the speed of information transmission without the necessary power of the radio link and signal processing algorithms will not give a tangible effect when transmitting information in difficult conditions.

REFERENCES

1. Definition of cognitive radio system. Report ITU-R SM.2152 09/2009. Electronic Publication. Geneva. 2009. P. 2. URL: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2152-2009-PDF-E.pdf (date of access 09.10.2018).

2. Miroshnik I.V., Nikiforov V.O., Fradkov A.L. *Nelinejnoe i adaptivnoe upravlenie slozhnymi sistemami* [Nonlinear and adaptive control of complex systems]. St. Petesberg: Nauka, 2000. 549 p. (In Russian)

3. Gorodeckij V.I. Mnogoagentnye sistemy: sovremennoe sostoyanie issledovaniy i perspektivy [Multi-agent systems: current state of research and prospects]. *Novosti iskusstvennogo intellekta* [Artificial intelligence news]. 1996. No. 1. Pp. 44–59. (In Russian)

4. Saaty T.L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation (Decision Making Series)*. New York: McGraw-Hill, 1980. 287 p.

5. Saaty R.W. The Analityc Hierarchy Process – What it is and How it is Used. *Mathematical Modelling*. 1987. Vol. 9(3–5). Pp. 161–176.

6. Quyen Nlhtt, Nguyen P.T., Huynh V.D.B., A hybrid multi criteria decision analysis for engineering project manager evaluation. *International Journal of Advanced and Applied Sciences*. 2017. Vol. 4. No. 4. Pp. 49–52.

7. Lambert J.M. The Extended Analytic Hierarchy Decision Method. *Mathematical and Computer Modelling*. 1991. Vol. 15(11). Pp. 141–151.

8. Ho W., Ma X., The State-of-the-art Integrations and Applications of the Analytic Hierarchy Process. *European Journal of Operational Research*. 2017. URL: https://doi.org/10.1016/j.ejor.2017.09.007 (date of access 10.10.2018).

9. Ivanco M., Hou G., Michaeli J. Sensitivity Analysis Method to Address User Disparities in the Analytic Hierarchy Process. *Expert Systems with Applications*. 2017. Vol. 90. Pp. 111–126.

10. Alberto A. Aguilar-Lasserre, Marco A. Bautista Bautista, Antonin Ponsich, Magno A. González Huerta. An AHP-based decision-making tool for the solution of multiproduct batch plant design problem under imprecise demand. *Computers & Operations Research*. 2009. Vol. 36. Issue 3. Pp. 711–736. ISSN0305-0548. URL: https://doi.org/10.1016/j.cor.2007.10.029 (date of access 10.10.2018).

11. Alessio Ishizaka, Ashraf Labib. Review of the main developments in the analytic hierarchy process. *Expert Systems with Applications*. 2011. No. 38. Pp. 14336–14345, http://dx.doi.org/10.1016/j.eswa.2011.04.143 (date of access 10.10.2018).

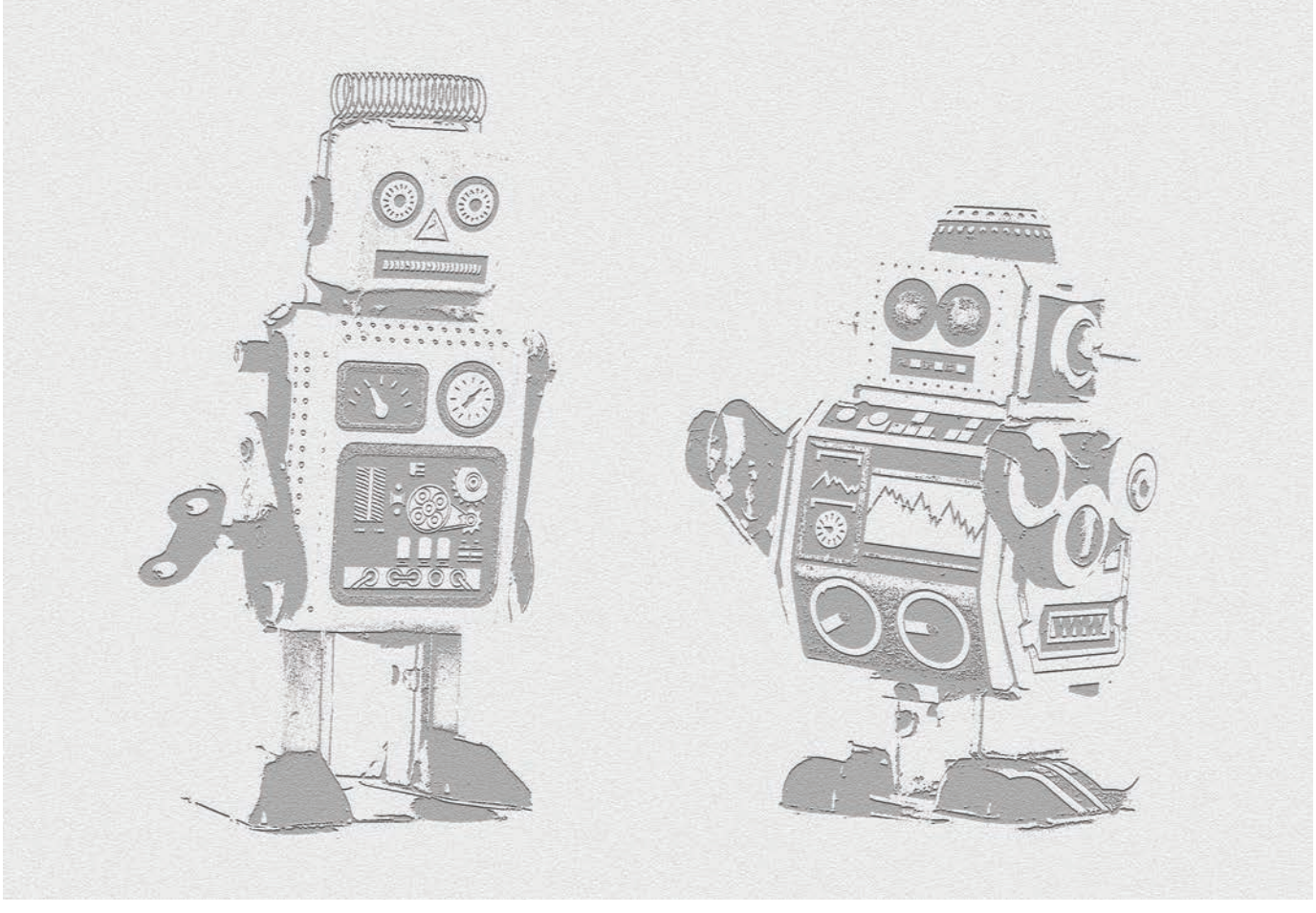
12. Zhirov D.K. Automatic Control System of Multi-Component Materials Processing and Its Operations Analysis by Final Product

Quality Criterion. *Bulletin of Kalashnikov ISTU*. 2011. No. 4 (52). Pp. 132–135. (In Russian)
13. Blagodatskij G. A. Application of Saati Method of Hierarchy Analysis to Accreditation Indexes of Higher School. *Bulletin of Kalashnikov ISTU*. 2010. No. 2 (46). Pp. 115–118. (In Russian)
14. Perevedentcev D.A. Modelling the system of fuzzy logical inference for evaluating science-intensive projects. *Automation of control processes*. 2017. No. 2 (46). Pp. 84–91. (In Russian)
15. Gorohov M.M**.** Development of Programming Tool for Estimating the Training Level of Higher Qualification Athletes. *Bulletin of Kalashnikov ISTU*. 2016. No. 2(70). Pp. 87–90. (In Russian)
16. Blagodatskij G.A. *Programmno-instrumental'nye sredstva povyshenija jeffektivnosti vnutrennih biznes-processov predprijatij* [Software instrumental tools to grow effectiveness of inner business-processes of enterprises]. Izhevsk: Kalashnikov Izhevsk State Technical University Publ., 2015. 188 p. (In Russian)
17. Kalitkin N.N. *Chislennye metody* [Numerical Methods]. Moscow: Nauka, 1978. Pp. 190–191. (In Russian)

INFORMATION ABOUT AUTHORS:

Blagodatsky G.A., PhD, Docent, Associate Professor at the Department of Information Systems of the Izhevsk State Technical University;
Kopysov A.N., PhD, Docent, Head of the Department of the Department of Radio Engineering of the Izhevsk State Technical University;
Khvorenkov V.V., PhD, Full Professor, Professor at the Department of Radio Engineering of the Izhevsk State Technical University;
Baturin I.S., postgraduate student of the Izhevsk State Technical University.

For citation: Blagodatsky G.A., Kopysov A.N., Khvorenkov V.V., Baturin I.S. Analysis of the hierarchical model of the automated control system of the parameters of the radio lines of the cognitive radio system. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 51–67. doi: 10.24411/2409-5419-2018–10187 (In Russian)



doi: 10.24411/2409-5419-2018-10188

ДОВЕРЕННЫЕ СИСТЕМЫ ДЛЯ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

ПАРАЩУК
Игорь Борисович[1]

САЕНКО
Игорь Борисович[2]

ПАНТЮХИН
Олег Игоревич[3]

АННОТАЦИЯ

Обоснованы актуальность и объективная необходимость повышения защищенности облачных инфраструктур критически важных информационных систем. Сформулированы ключевые понятия и подходы к построению современных средств обеспечения доверенной среды, построению доверенной платформы, организации доверенных сеансов и доверенной загрузки в интересах разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем. Проанализирована роль различных средств доверенной загрузки в структуре системы защиты облачных технологий и функции, реализуемые ими для разных уровней архитектуры автоматизированного рабочего места администратора или пользователя облачных технологий. Предметом исследования является роль и место систем, комплексов, модулей и иных средств доверенной загрузки в разграничении доступа и в обеспечении информационной безопасности облачных технологий и потенциал их применения. Целью работы является выработка единых понятийных взглядов и методологических подходов к построению доверенных систем, платформ, сеансов и средств доверенной загрузки в интересах разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем. Исследованы общие характеристики средств (модулей) доверенной загрузки, реализующих алгоритмы идентификации и аутентификации пользователей, регистрации действий пользователей и программ, алгоритмы блокировки. Исходя из современных требований к безопасности облачных технологий, предложен вариант состоятельной и безызбыточной системы параметров, характеризующих качество современных средств доверенной загрузки. Предлагается, чтобы в состав данной системы обязательно вошли параметры, учитывающие уровень защиты средств доверенной загрузки, их производительность, надежность, устойчивость функционирования, эргономичность, а также затраты (ресурсопотребление) на установку и эксплуатацию данных средств. Практическая значимость: существенным практическим аспектом предложенного подхода является тот факт, что существующие типы средств доверенной загрузки предназначены каждый для конкретных целей и для конкретных уровней защищаемых элементов облачных технологий, их применение должно осуществляться комплексно, с учетом уровня существующих угроз. При этом выбор средств доверенной загрузки должен осуществляться с учетом их показателей качества.

КЛЮЧЕВЫЕ СЛОВА: облачная инфраструктура; доверенная система; доверенная загрузка; операционная система; параметры; безопасность; разграничение доступа.

Сведения об авторах:

[1]д.т.н., профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия, shchuk@rambler.ru

[2]д.т.н., профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия, ibsaen@mail.ru

[3]к.т.н., доцент, доцент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, p_oleg99@mail.ru

Для цитирования: *Паращук И. Б., Саенко И. Б., Пантюхин О. И.* Доверенные системы для разграничения доступа к информации в облачных инфраструктурах // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 68–75. doi: 10.24411/2409-5419-2018-10188

Новый этап развития в области облачных технологий показал очевидность того, что для их внедрения в критически важные информационные системы необходима надежная система информационной безопасности. Необходимы современные механизмы разграничения доступа, нужно обеспечить надежную защиту облачных инфраструктур критически важных информационных систем от несанкционированного доступа (НСД). При этом информационная безопасность составляет основу всей системы безопасности облачных технологий. Именно она позволяет обеспечивать конфиденциальность, целостность и доступность информации в рамках облачных инфраструктур критически важных информационных систем. Информационная безопасность облачных инфраструктур характеризуется отсутствием недопустимого риска, связанного с утечкой информации из «облаков» вследствие НСД.

При организации информационной защиты облачных инфраструктур от НСД необходимо организовать пространство для надежного и безопасного функционирования этих технологий — создать доверенную среду (доверенную вычислительную или программно-аппаратную среду) [1]. В рамках понятия «доверенности» предполагается, что есть некий объект — система или процесс (среда, окружение, платформа, сеанс, загрузка), в поведении которых пользователь облачных технологий полностью уверен. Это объект, которому пользователь может доверять на сто процентов. Ожидаемое поведение данного объекта всегда совпадает с реальным. Понятие основано на фразеологизме «корень доверия» — от английского Root of Trust (набор компонентов, которым можно доверять). Таким образом, «доверенность» — гарантированное, строгое соответствие актуальным требованиям в части информационной безопасности облачных технологий, в части надежности и функциональной устойчивости в условиях современного информационного противоборства, но, при соблюдении определенных условий технологической независимости. Доверенная система облачных технологий — система, которая использует доверенные аппаратные и программные средства для разграничения привилегий абонентов облачных инфраструктур и обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа [2].

Исходя из этого, можно сформулировать понятие «доверенная среда» (доверенная вычислительная или программно-аппаратная среда) облачных технологий. Это взаимоувязанная по времени и задачам совокупность систем и средств разграничения доступа, идентификации и аутентификации, межсетевых экранов, средств антивирусной защиты и криптографических стандартов. Она отвечает политике безопасности и создает защищенное «облачное пространство». Для формирования такой среды необходимо выполнение двух основных условий: первое — вся аппаратная часть облачных инфраструктур должна быть полностью досконально проверена и перепроверена или создана самостоятельно на отечественной элементной базе. Второе — все программные средства, созданные для работы на этом оборудовании, должны быть написаны самостоятельно либо тщательно, детально и «придирчиво» проверены.

Таким образом, доверенная среда облачных инфраструктур — некое информационно-техническое, киберфизическое пространство, сформированное на основе комплекса технических и организационных мер и способное обеспечить его участникам предсказуемый и безопасный результат информационного взаимодействия. Важно, что при этом степень доверенности среды определяется надежностью циркулирующего в ней и предоставляемого ею контента [2]. В рамках доверенной среды (доверенной вычислительной среды) облачных инфраструктур используются модули доверенной загрузки и средства разграничения доступа с динамическим контролем целостности данных. Известно, что абсолютное большинство современных компьютеров и серверов, использующихся в облачных инфраструктурах, трудно, почти невозможно назвать доверенными. Всегда сохраняется потенциальная угроза доступа нарушителя к компьютерам и другим электронным устройствам облачных инфраструктур, к их программному обеспечению (ПО), используя предварительно созданные и «глубоко запрятанные» (в процессе создания облачных инфраструктур) программные и аппаратные искусственные уязвимости, «закладки». Такие «закладки» могут находится как на вычислительных устройствах, так и на устройствах памяти и ввода-вывода элементов и средств облачных инфраструктур. Считается, что доверенная среда включает в себя [3]: доверенное аппаратное обеспечение (элементная база отечественного производства и отечественные аппаратные средства защиты информации), доверенное программное обеспечение (проверенное или отечественное системное ПО, прикладное ПО и программные средства защиты от НСД), выверенные и апробированные политики безопасности, доверенные каналы передачи, а также доверенное окружение и пользователи облачных инфраструктур.

Под доверенным окружением для облачных инфраструктур обычно понимают взаимосвязанную совокупность [3]: доверенных средств связи (стационарных и мобильных), доверенных механизмов сетевой безопасности, доверенных платформ визуализации и виртуализации, доверенных алгоритмов аутентификации пользователей, средств (оборудования) обеспечения этой безопасности, доверенных механизмов и средств облачных вычислений и хранения данных, доверенных программных средств и программных приложений (операционных систем, библиотек, web-сервисов, программных средств аутентифи-

кации и защиты данных и др.), доверенных устройств печати и копирования, доверенных серверов и рабочих мест пользователей облачных технологий.

Создание «доверенной платформы» (доверенной вычислительной или программно-аппаратной платформы) для облачных инфраструктур заключается в использовании отечественных комплексов оборудования для обеспечения устойчивости критически важных информационных систем и защиты информации. При этом принято считать, что составными частями доверенной платформы могут выступать: аппаратное обеспечение, программное обеспечение и элементная база. Поэтому задача, стоящая перед создателями доверенной платформы для облачных инфраструктур, состоит в обеспечении отечественных организаций и предприятий аппаратными и программными средствами, которые гарантируют защищенность и отсутствие недокументированных (незадекларированных) возможностей (НЗДВ) внутри оборудования и ПО облачных технологий [3].

На уровне ПО доверенная платформа облачных технологий (доверенные программные компоненты) включает в себя: пользовательское ПО (защищенное ПО для пользователей облачных технологий), системное ПО (защищенную базовую систему ввода-вывода) и серверное ПО (защищенное ПО для серверов облачной инфраструктуры). Доверенное оборудование облачных технологий — компьютерные и телекоммуникационные средства, созданные на основе доверенного встроенного ПО, собранные из элементов доверенной элементной базы доверенными, лучше отечественными, производителями. Доверенная элементная база облачных технологий предопределяет, что компьютерные и телекоммуникационные средства должны гарантировать защищенность и отсутствие НЗДВ внутри электронных компонентов. Понятие «доверенный сеанс» облачных технологий (сеанс связи) в литературе и Руководящих документах трактуется как период работы компьютерных и телекоммуникационных средств с доступом к облачным сервисам, в рамках которого осуществляется защищенное соединение, обеспечивается доверенная загрузка операционной системы (ОС) и обязательно поддерживаются такие условия работы, которые гарантируют защищенность (например, с применением электронной цифровой подписи). Термин «доверенная загрузка» описывает функцию (способность, свойство) персонального компьютера, иных вычислительных и телекоммуникационных средств облачных технологий, для воспрепятствования несанкционированному запуску их пользователем, загрузке ОС и получению возможности доступа к конфиденциальной информации облачных инфраструктур [2]. Принято считать, что доверенная загрузка относится к одному из направлений внешних средств защиты от НСД в рамках облачных технологий, вместе со средствами контроля работоспособности, контроля целостности, компонентами разграничения и защиты доступа к внутренним элементам технических средств и средствами работы с внешними носителями.

Известны различные подходы к формулировке понятия «доверенная загрузка». Так, например, под доверенной загрузкой понимают применение программных и программно-технических средств, используемых в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом и реализующих функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки [4]. Довольно часто под доверенной загрузкой понимается загрузка ОС с внутреннего жесткого диска компьютера. Эта загрузка происходит только после проверки целостности программной и аппаратной среды (в том числе, целостности объектов загружаемой ОС), только после выполнения процедур идентификации и аутентификации пользователя облачных технологий. При этом должна обеспечиваться невозможность загрузки пользователем облачных технологий другой ОС (с внешних носителей информации и др.) [5].

Иногда под доверенной загрузкой понимают загрузку различных ОС исключительно с заранее определенных постоянных носителей (например, только с конкретного жесткого диска). И только после успешного завершения специальных процедур — процедур проверки (верификации) пользователя и процедур проверки целостности технических и программных средств персонального компьютера (ПК) или иных вычислительных и телекоммуникационных средств с доступом к облачным сервисам. Это осуществляется с использованием механизма пошагового контроля целостности, а также аппаратной идентификации и аутентификации пользователя облачных технологий [6]. Другими словами, в этом режиме загрузка различных ОС ПК либо иных вычислительных и телекоммуникационных средств с доступом к облачным сервисам осуществляется только в том случае, если подтверждено, что в них не произошло никаких несанкционированных изменений (на аппаратном уровне и в критичной части приложений) и что включает их именно тот пользователь, который имеет право на нем работать именно в это время [7].

Процесс доверенной загрузки ПК пользователя, либо иных вычислительных и телекоммуникационных средств с доступом к облачным сервисам, в рамках процедур разграничения доступа к информации в облачных инфраструктурах необходим для того, чтобы воспрепятствовать несанкционированному запуску этих устройств, загрузке операционной системы и получению возможности доступа к конфиденциальной информации, хранящейся в «об-

лаке». При этом в сферу действия средств доверенной загрузки входят этапы работы компьютера или другого терминала пользователя от запуска микропрограммы базовой системы ввода-вывода — BIOS (Basic Input Output System) до начала загрузки операционной системы [6]. В этом случае доверенная загрузка включает в себя аутентификацию пользователя; контроль устройства (жесткого диска или другого носителя), с которого BIOS начинает загрузку ОС; контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой ОС; шифрование и дешифрование загрузочного сектора, системных файлов ОС, либо шифрование всех данных устройства, а также аутентификацию, шифрование и хранение режимных (конфиденциальных) данных, таких как ключи и контрольные суммы [6].

Принято различать три основных типа средств доверенной загрузки [4, 7]: средства доверенной загрузки уровня базовой системы ввода-вывода; средства доверенной загрузки уровня платы расширения (программно-аппаратные средства доверенной загрузки); средства доверенной загрузки уровня загрузочной записи. При этом для дифференциации требований к функциям безопасности средств доверенной загрузки выделяются шесть классов защиты средств доверенной загрузки. Самый низкий класс — шестой, самый высокий — первый [4]. Средства доверенной загрузки уровня базовой системы ввода-вывода обычно тесно интегрированы с прошивкой материнской платы, активируются прямым вызовом из базовой системы ввода-вывода, пользуются всеми защитными функциями контроллера доступа к внутренней памяти, не требуют дополнительных затрат на установку и эксплуатацию, при покупке обходятся дешевле по сравнению с программно-аппаратными устанавливаемыми решениями [7–8]. Программно-аппаратные средства доверенной загрузки обычно устанавливаются на плату (шину) расширения и позволяют, при подаче питания на устройство и получении управления, выполнять контроль целостности конфигурации и логических объектов на накопителях данных [4, 7]. Средства доверенной загрузки уровня загрузочной записи являются решением, обеспечивающим (в большей степени) недоступность пользовательских данных с помощью нестандартного форматирования и (или) шифрования носителя этих данных [7]. Иногда их называют модулями доверенной платформы TPM — Trusted Platform Module [9–10].

Рассмотрим типовые угрозы и параметры, характеризующие существенные свойства современных средств доверенной загрузки для разграничения доступа к информации в облачных инфраструктурах.

К базовому перечню угроз, которые должны быть нейтрализованы средствами доверенной загрузки относят [11–18]: нарушение целостности программной среды средств облачной инфраструктуры и (или) состава компонентов аппаратного обеспечения средств для реализации облачных технологий; несанкционированная загрузка штатной операционной системы и получение несанкционированного доступа к ресурсам облачных технологий; загрузка нештатной ОС для обхода правил разграничения доступа штатной ОС и (или) других средств защиты информации, работающих в среде штатной ОС облачных технологий.

Выбор конкретного средства доверенной загрузки определяется в результате детального анализа этих угроз и на основе выработки политики защиты облачных технологий от НСД. Зачастую, когда говорят о программно-аппаратных средствах доверенной загрузки, имеют ввиду, так называемые, модули доверенной загрузки. Такие модули представляют собой комплексы аппаратно-программных средств, устанавливаемые (встраиваемые) в компьютер (сервер, ноутбук, специализированный компьютер и др.) и обеспечивающие контроль доступа пользователя облачных технологий к рабочему месту, а также контроль целостности программной среды рабочего места и программной среды облачной инфраструктуры [5].

На автоматизированном рабочем месте пользователя типовой модуль доверенной загрузки должен обеспечивать выполнение следующих основных функций: регистрацию действий как пользователей, так и программ; блокировку несанкционированной загрузки ОС с внешних съемных носителей; идентификацию и аутентификацию пользователей до загрузки ОС с помощью персональных электронных идентификаторов; контроль целостности объектов системы, объектов пользователя и программного обеспечения модуля доверенной загрузки до загрузки ОС; предоставление возможностей для внешних приложений (работа с датчиком случайных чисел, работа с электронными идентификаторами и т. д.) [5].

При работе в рамках облачной инфраструктуры осуществляется первичная настройка модуля доверенной загрузки (МДЗ). Это, по сути, назначение администратора модуля, который обладает привилегиями на регистрацию и удаление пользователей, управление параметрами работы модуля, просмотр журнала событий и управление списком объектов, целостность которых должна контролироваться до загрузки операционной системы. В некоторых модулях доверенной загрузки реализована поддержка возможности удаленного управления параметрами работы. В случае появления нарушений при проверке целостности объектов возможность работы на компьютере для обычных пользователей блокируется.

Как правило, МДЗ реализуются на базе плат с системными шинами, которые могут включать следующие компоненты:

– микросхема flash-памяти с программным расширением BIOS компьютера, которое получает управление

до старта операционной системы и обеспечивает выполнение основных функций МДЗ;

– программируемая логическая интегральная схема (для реализации интерфейса по шине и выполнения функций по работе с другими компонентами платы) и микросхема памяти для хранения кода загрузчика интегральной схемы;

– микросхема микроконтроллера для защищенной реализации специальных функций модуля (например, для взаимодействия с некоторыми компонентами платы или для кода, выполнение которого не в центральном процессоре компьютера повышает его защищенность от перехвата и модификации злонамеренными программами);

– энергонезависимая память, предназначенная для хранения настроек МДЗ, журналов событий и других данных;

– блок управления сторожевым таймером (watch dog), который не позволяет работать с компьютером в случае, если программное расширение BIOS модуля не получило управления. Данный механизм не позволит получить доступ к компьютеру посредством специальной настройки параметров BIOS или в случае системного сбоя;

– датчик случайных чисел, необходимый для аппаратной выработки последовательностей случайных величин;

– блок часов реального времени, предназначенный для независимого замера времени с целью обеспечения защищенной реализации механизмов периодического устаревания критичных данных, а также других функций МДЗ;

– разъемы различных типов для подключения электронных идентификаторов (iButton, USB);

– переключатели для изменения режимов работы МДЗ [5, 8].

Помимо этого, в состав МДЗ может входить программное обеспечение для поддерживаемых ОС, которое обычно включает драйвер, программу управления и интерфейсный модуль для внешних приложений. Современные МДЗ поддерживают работу на компьютерах как с ОС семейства MS Windows, так и с рядом ОС семейства UNIX/Linux [5].

Параметрами МДЗ будем считать количественную характеристику одного или нескольких свойств этих средств, рассматриваемую применительно к определенным условиям их создания и эксплуатации. При этом к базовым свойствам, определяющим качество средств доверенной загрузки, можно отнести [19]: уровень защиты; производительность; надежность; устойчивость; эргономичность; затраты (ресурсопотребление) на установку и эксплуатацию средств доверенной загрузки.

Параметрами, количественно характеризующими эти свойства можно считать конкретные параметры (вариант):

Для уровня защиты средств доверенной загрузки: количество отражаемых типов НСД; уровень идентификации и аутентификации должностных лиц; уровень проверки целостности ОС.

Для контроля производительности средств доверенной загрузки: интенсивность отраженных попыток НСД (попытка/сек.); время реакции на попытку НСД (сек.); время задержки реакции на попытку НСД (сек.).

Для контроля надежности средств доверенной загрузки: время безотказной работы средства доверенной загрузки (час); время замены (без настройки) средства доверенной загрузки в случае выхода из строя (мин.).

Для контроля устойчивости средств доверенной загрузки: время восстановления после пограничных сбоев (сек.); количество видов воздействия, которым может противостоять средство доверенной загрузки.

Для контроля эргономичности средств доверенной загрузки: время увеличения загрузки автоматизированного рабочего места пользователя (сек.); время, необходимое на полную настройку одного комплекта средств доверенной загрузки (сек.); время, необходимое на смену ключевой информации одного комплекта средств доверенной загрузки (сек.).

Для контроля затрат (ресурсопотребления) на установку и эксплуатацию средств доверенной загрузки: стоимость приобретения одного комплекта средств доверенной загрузки (руб.); затраты на эксплуатацию комплекта средств доверенной загрузки (руб.); затраты производительности автоматизированного рабочего места пользователя, необходимой для функционирования комплекта средств доверенной загрузки (Кбит/сек.).

Набор этих параметров представляет собой систему показателей качества средств доверенной загрузки. Однако, появились новые угрозы безопасности облачных технологий, мир компьютерных угроз пополнился новыми способами проникновения, использующими аппаратные уязвимости современных вычислительных платформ. Такие угрозы связаны с появлением новых вредоносных программ, размещаемых на уровне ядра операционной системы, с появлением новых загрузочных программных модулей. И сейчас, на современном этапе для борьбы с такими вредоносными программами нужно иметь средства контроля состояния файловой системы и сканирования пространства оперативной памяти [5]. Вместе с тем, сегодня большинство аппаратных решений не поддерживаются операционными системами. Это приводит к появлению новых компьютерных уязвимостей и значительному повышению вероятности реализации злонамеренных действий, не контролируемых со стороны ОС. Проникновение и функционирование современных вредоносных программных модулей, выполняемых микроконтроллером, никак не контролируется средствами ОС и антивирусными программами. Поэтому имеется возможность глобального скрытого контроля над компьютером, над облачной инфраструк-

турой из любой точки мира через сеть Интернет [5]. Эти пути проникновения вредоносных программ и сами программы в настоящий момент не могут быть обнаружены и блокированы традиционными способами.

Для обеспечения надежного контроля ресурсов облачных технологий и их параметров безопасности необходимо наблюдать и оценивать состояние: аппаратуры виртуализации; содержимого микросхем энергонезависимой памяти системной платы; параметров распределения памяти; настроек контроллеров; периферийных расширений BIOS на внешних адаптерах. Осуществление такого наблюдения и оценивания можно возложить на независимые аппаратные средства, вынесенные за пределы области управления и контроля со стороны потенциально опасной аппаратуры и программного кода. В качестве такого устройства иногда [5] предлагается использовать средства доверенной загрузки, дополнив их специальными модулями контроля аппаратной платформы.

Таким образом, рассмотрены сущность и содержание понятия «доверенность», связанного с проблемами обеспечения защиты информации, задачами разграничения доступа к информации в облачных инфраструктурах с использованием программно-аппаратной системы, платформы, среды или средств. Рассмотрены сущность и содержание понятий доверенная среда, доверенная платформа, доверенный сеанс и доверенная загрузка в рамках обеспечения информационной безопасности облачных технологий. Определено, что существующие типы средств доверенной загрузки предназначены каждый для конкретных целей и для конкретных уровней защищаемых элементов облачных технологий, их применение должно осуществляться комплексно, с учетом уровня существующих угроз. При этом выбор средств доверенной загрузки должен осуществляться с учетом их показателей качества [20].

Очевидно, что роль комплексов, модулей и иных средств доверенной загрузки в разграничении доступа и в обеспечении информационной безопасности облачных технологий достаточно велика и потенциал их применения объективно возрастает. Это системы, позволяющие без больших финансовых затрат, оперативно и гарантированно предотвращать несанкционированный доступ к программным и техническим ресурсам средств сбора, обработки, хранения и передачи информации в облачных инфраструктурах.

Предложен вариант формулировки параметров современных средств доверенной загрузки — надежных, простых в администрировании и сравнительно недорогих средств разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем.

Исследование было поддержано грантом РФФИ (проект № 18–07–01369) в СПИИРАН.

Литература

1. *Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В.* Доверенная среда — основа гарантированной безопасности // Информационная безопасность. 2013. № 2. Pp. 36–37.

2. *Вернер О.В.* Эволюция подхода к построению доверенной среды. URL: http://elvis.ru/upload/iblock/53e/verner_trusted-env.pdf (дата обращения 07.10.2018).

3. *Буров А.С.* Перспективы создания доверенной платформы. URL: http://www.altell.ru/about/ press-centre/news/АльтЭль%2020Перспективы%20создания%20доверенной%20платформы.pdf (дата обращения 07.10.2018).

4. *Авезова Я.Э., Фадин А.А.* Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1 (14). С. 24–30.

5. *Никитин Е.А., Шрамко В.А.* Всегда ли на замке? Как обезопасить компьютер модулем доверенной загрузки // Системный администратор. Приложение «Безопасность». 2010. № 2(2). URL: http://samag.ru/archive/article/1068 (дата обращения 07.10.2018).

6. *Конявский В.А.* Управление защитой информации на базе СЗИ НСД «Аккорд». М.: Радио и связь, 1999. 325 с.

7. Модули доверенной загрузки. URL: http://labvs.ru/moduli-doverennoj-zagruzki/ (дата обращения 07.10.2018).

8. *Левенков О.А.* Средства доверенной загрузки // Технологии безопасности. 2013. № 6. С. 40.

9. *Tomlinson A.* Introduction to the TPM. // Smart Cards, Tokens, Security and Applications:. London: Springer-Verlag London Limited, 2008. pp. 155–172.

10. *Gallery E., Mitchell C.J.* Trusted Computing: Security and Applications // Cryptologia. 2008. Vol. 33. Pp. 217–245.

11. *Sattarova F.Y., Kim T.H.* IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. // International Journal of Multimedia and Ubiquitous Engineering. 2007. Vol. 2. No. 2. Pp. 17–31.

12. *Allsopp W.* Unauthorised Access. New York: John Wiley & Sons. 2010. 302 p.

13. *Ahonen P., Eronen J., Holappa J., Kajava J., Kaksonen T., Karjalainen K., Karppinen K., Rapeli M.,. Röning J, Sademies A., Savola R., Uusitalo I., Wiander T.* Information security threats and solutions in the mobile world. The service developerís perspective. Espoo. Finland: Espoo, 2005. 95 p.

14. *Rasmi M., Jantan A.* Attack Intention Analysis Model for Network Forensics // Software Engineering and Computer Systems. 2011. Pp. 403–411.

15. *Arfa Rabai L.B., Jouini M., Aissa A.B., Mili A.* A cybersecurity model in cloud computing environments // Journal of King Saud University — Computer and Information Sciences. 2012. No. 1. Pp. 63–75.

16. *Jouini M., Arfa Rabai L.B., Aissa A.B., Mili A.* Towards quantitative measures of Information Security: A Cloud Computing case study // International Journal of Cyber-Security and Digital Forensics (IJCSDF). 2012. No. 1(3). Pp. 265–279.

17. *Arfa Rabai L. B., Jouini M., Aissa A. B., Mili A.* An economic model of security threats for cloud computing systems // International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). 2012. Pp. 100–105.

18. *Arnold T.* A Comparative Analysis Of Rootkit Detection Techniques // Computer Science and Engeneering. 2011. Pp. 8–16.

19. *Паращук И.Б., Логинов В.А., Елизаров В.В.* Оптимизация пространства параметров IT-инфрас-труктуры, оцениваемых SIEM-системой в условиях неопределенности // Информация и космос. 2018. № 1. С. 75–80.

20. *Паращук И.Б., Башкирцев А.С., Саяркин А.Л.* Вариант формулировки показателей качества современных средств доверенной загрузки и их роль при решении проблем безопасности алгоритмов управления инфотелекоммуникационными системами специального назначения // Вопросы оборонной техники. Серия 16. 2016. № 95–96. С. 47–51.

TRUSTED SYSTEMS TO DIFFERENTIATE ACCESS TO INFORMATION IN CLOUD INFRASTRUCTURES

IGOR B. PARASHCHUK,
Saint-Petersburg, Russia, shchuk@rambler.ru

IGOR B. SAENKO,
Saint-Petersburg, Russia, ibsaen@mail.ru

OLEG I. PANTJUHIN,
Saint-Petersburg, Russia, p_oleg99@mail.ru

KEYWORDS: cloud infrastructure; trusted system; trusted boot; operating system; settings; security; differentiate access.

ABSTRACT

The urgency and objective need to improve the security of cloud infrastructure of critical information systems are substantiated. The key concepts and approaches to the construction of modern means of providing a trusted environment, the construction of a trusted platform, the organization of trusted sessions and trusted downloads in order to differentiate access to information in the cloud infrastructure of critical information systems are formulated. The role of various trusted boot tools in the structure of the cloud technologies protection system and the functions implemented by them for different levels of the automated workplace architecture of the administrator or user of cloud technologies are analyzed. The subject of the research is the role and place of systems, complexes, modules and other means of trusted loading in access control and information security of cloud technologies and their potential application. The aim of the work is to develop common conceptual views and methodological approaches to the construction of trusted systems, platforms, sessions and trusted download tools in order to differentiate access to information in the cloud infrastructure of critical information systems. The General characteristics of the means (modules) of trusted loading, implementing algorithms of identification and authentication of users, registration of actions of users and programs, algorithms of blocking are investigated. Based on the modern requirements for the security of cloud technologies, a variant of a well-established and unprofitable system of parameters characterizing the quality of modern means of trusted download is proposed. It is proposed that the structure of this system necessarily includes parameters that take into account the level of protection of trusted boot facilities, their performance, reliability, stability of operation, ergonomics, as well as costs (resource consumption) for the installation and operation of these facilities. Practical value: an essential practical aspect of the proposed approach is the fact that the existing types of trusted boot tools are designed for each specific purpose and for specific levels of protected elements of cloud tech-

nologies, their use should be carried out in a comprehensive manner, taking into account the level of existing threats. In this case, the choice of trusted boot tools should be based on their quality indicators.

REFERENCES

1. Borodakij Y.V., Dobrodeev A.Y., Butusov I.V. Doverennaya sreda – osnova garantirovannoj bezopasnosti [Trusted environment-the Foundation of guaranteed security]. *Information Security*. 2013. No. 2. Pp. 36–37. (In Russian)

2. Verner O.V. Ehvolyuciya podhoda k postroeniyu doverennoj sredy [The evolution of the approach to building a trusted environment]. URL: http://elvis.ru/upload/iblock/53e/verner_trusted-env.pdf (date of access 07.10.2018). (In Russian)

3. Burov A.S. Perspektivy sozdaniya doverennoj platform [Prospects for creating a trusted platform]. URL: http://www.altell.ru/about/press-centre/news/Al'tEHl'%2020Perspektivy%20sozdaniya%20doverennoï%20platformy.pdf. (date of access 07.10.2018). (In Russian)

4. Avezova Y.E., Fadin A.A. Issues of Trusted Boot in Physical and Virtual Environments. *Voprosy kiberbezopasnosti*. 2016. No. 1 (14). Pp. 24–30. (In Russian)

5. Nikitin E.A., Shramko V.A. Vsegda li na zamke? Kak obezopasit' komp'yuter modulem doverennoj zagruzki [Always locked up? How to secure your computer with a trusted boot module]. *Sistemnyy administrator. Prilozhenie "Bezopasnost'"* [System administrator. Annex "Security"]. 2010. No. 2(2). URL: http://samag.ru/archive/article/1068. (date of access 07.10.2018). (In Russian)

6. Konyavskij V.A. *Upravlenie zashchitoj informacii na baze SZI NSD "Akkord"* [Management of information security on the basis of szi NSD "Accord"]. Moscow: Radio i svyaz', 1999. 325 p. (In Russian)

7. Moduli doverennoj zagruzki [Trusted boot modules]. URL: http://labvs.ru/moduli-doverennoj-zagruzki/ (date of access 07.10.2018). (In Russian)

8. Levenkov O.A. Sredstva doverennoj zagruzki [Trusted download tools]. *Tekhnologii bezopasnosti* [Security technology].2013. No. 6. Pp. 40. (In Russian)

9. Tomlinson A. Introduction to the TPM. Smart Cards, Tokens, Security and Applications. London: Springer-Verlag London Limited, 2008. Pp. 155–172.

10. Gallery E., Mitchell C.J. Trusted Computing: Security and Applications. *Cryptologia*. 2008. Vol. 33. Pp. 217–245.

11. Sattarova F.Y., Kim T.H. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*. 2007. Vol. 2. No. 2. Pp. 17–31.

12. Allsopp W. *Unauthorised Access***.** New York: John Wiley & Sons. 2010. 302 p.

13. Ahonen P., Eronen J., Holappa J., Kajava J., Kaksonen T., Karjalainen K., Karppinen K., Rapeli M.,. Röning J, Sademies A., Savola R., Uusitalo I., Wiander T. *Information security threats and solutions in the mobile world. The service developerís perspective*. Espoo. Finland: Espoo, 2005. 95 p.

14. Rasmi M., Jantan A. Attack Intention Analysis Model for Network Forensics. *Software Engineering and Computer Systems*. 2011. Pp. 403–411.

15. Arfa Rabai L.B., Jouini M., Aissa A.B., Mili A. A cybersecurity model in cloud computing environments. *Journal of King Saud University – Computer and Information Sciences*. 2012. No. 1. Pp. 63–75.

16. Jouini M., Arfa Rabai L.B., Aissa A.B., Mili A. Towards quantitative measures of Information Security: A Cloud Computing case study. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*. 2012. No. 1(3). Pp. 265–279.

17. Arfa Rabai L.B., Jouini M., Aissa A.B., Mili A. An economic model of security threats for cloud computing systems. *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. 2012. Pp. 100–105.

18. Arnold T. A Comparative Analysis Of Rootkit Detection Techniques. *Computer Science and Engeneering*. 2011. Pp. 8–16.

19. Parashchuk I.B., Loginov V.A., Elizarov V.V. Optimizing IT-infrastructure parameter space being assessed by SIEM system under uncertainty. *Informaciya i kosmos* [Information and space]. 2018. No. 1. Pp. 75–80. (In Russian)

20. Parashchuk I.B., Bashkircev A.S., Sayarkin A.L. A variant of formulation of quantitative indices of modern means of confidence load and their role in security problems decision of control algorithms of special-purpose infotelecommunication systems. *Military Enginery. Counter-terrorism technical devices*. 2016. No. 95–96. Pp. 47–51. (In Russian)

INFORMATION ABOUT AUTHORS:

Parashchuk I.B., PhD, Full Professor, Leading Researcher of the St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences;

Saenko I.B., PhD, Full Professor, Leading Researcher of the St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences;

Pantjuhin O.I., PhD, Docent, Associate Professor of St. Petersburg state University of telecommunications prof. M.A. Bonch-Bruevich.

For citation: Parashchuk I.B., Saenko I.B., Pantjuhin O.I. Trusted systems to differentiate access to information in cloud infrastructures. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 68–75. doi: 10.24411/2409-5419-2018-10188 (In Russian)

doi: 10.24411/2409-5419-2018-10189

МЕТОДИКА ОЦЕНКИ УСТОЙЧИВОСТИ СЕТИ В УСЛОВИЯХ ТАРГЕТИРОВАННОЙ КИБЕРНЕТИЧЕСКОЙ АТАКИ

КОЦЫНЯК
Михаил Антонович[1]

СПИЦЫН
Олег Леонтьевич[2]

ИВАНОВ
Денис Александрович[3]

АННОТАЦИЯ

Эффективная и надежная защита компьютерной сети невозможна без предварительного анализа возможных угроз ее безопасности, среди которых наиболее сильными являются таргетированные компьютерные атаки. Таргетированные компьютерные атаки и способность противодействовать их реализации является ключевыми факторами, определяющими устойчивость компьютерных сетей. Оценка свойства устойчивости компьютерной сети в условиях таргетированных компьютерных атак, под которым понимается ее возможность противостоять различным видам пассивных и активных атак и сохранять показатели своего функционирования в условиях воздействия этих атак, является достаточно важной и сложной задачей. Аналитическое моделирование таргетированных компьютерных атак во многом помогает эффективному решению этой задачи. В работе предлагается применять метод преобразовании стохастических сетей для аналитического моделирования различных типов таргетированных компьютерных атак и использовать результаты моделирования для решения задачи оценки устойчивости компьютерной сети. Суть метода заключается в том, что исследуется не система, а целевой процесс который она реализует. Этот сложный процесс декомпозируется на элементарные процессы, каждый из которых может характеризоваться функцией распределения времени выполнения процесса, плотностью вероятности, вероятностью или средним и дисперсией времени выполнения. Этот подход отличается более высокой точностью и устойчивостью получаемых решений. Он хорошо зарекомендовал себя для моделирования многошаговых стохастических процессов различной природы. Расчет показателей устойчивости сети в условиях таргетированных кибернетических атак, осуществлялся через вероятностно-временные характеристики. Для этого разработаны рассмотрены физические основы реализации таргетированных компьютерных атак, разработаны профильные модели этапов воздействия таргетированных компьютерных атак и с помощью метода преобразования стохастических сетей рассчитаны вероятностно-временные характеристики всех этапов таргетированных компьютерных атак. Теоретический вклад работы заключается в дальнейшем развитии методов аналитического моделирования компьютерных атак и в их применении для оценки устойчивости как очень важного свойства компьютерной сети. Новизна полученных результатов определяется использованием метода преобразования стохастических сетей для аналитического моделирования компьютерных атак.

КЛЮЧЕВЫЕ СЛОВА: таргетированная кибернетическая атака; моделирование атак; защищенность компьютерной сети; стохастические сети; преобразование Лапласа.

Сведения об авторах:

[1]д.т.н., профессор, профессор Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, koc-1942@mail.ru

[2]к.т.н., преподаватель кафедры Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург,Россия, laos-82@yandex.ru

[3]адъюнкт Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия, prosto_deniss@mail.ru

Для цитирования: *Коцыняк М.А., Спицын О.Л., Иванов Д.А. Методика оценки устойчивости сети в условиях таргетированной кибернетической атаки* // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 76–85. doi: 10.24411/2409-5419-2018-10189

По мнению специалистов, в последнее время наблюдается смещение акцента с написания вредоносных программ на проведение таргетированных кибернетических атак (ТКА) [1]. Атаки направленны на определенную организацию, и подготовка к ним занимает много времени. Противники тщательно изучают используемые у потенциальной жертвы средства защиты и находят нужные уязвимости, которые используются для проведения атаки. Сегодня известно о более чем ста проводящих таргетированных кибернетических атак. От их действий страдают государственные и коммерческие структуры в 85 странах [2–4]. Такой широкое распространение объясняется оптимизацией средств взлома, что проводит к упрощению и удешевлению проведения вредоносных операций.

Таргетированная кибернетическая атака на элементы информационно-телекоммуникационную сеть (ИТКС) реализуется в виде несанкционированного активного процесса в инфраструктуре сети, удаленно управляемая в реальном масштабе времени, с целью нарушения или снижения эффективности выполнения технологических циклов.

Процесс функционирования комплекса ТКА включает функции [5]:

1. Подготовительную.
2. Разработки набора инструментов.
3. Несанкционированный доступ.

Процесс реализации воздействия ТКА начинается с подготовительной функции, который включает в себя (рис. 1):

– поиска (сетевого сканирования);
– создания стенда воздействия;
– обхода стандартных средств защиты;
– поиска (сетевого сканирования).

Подсистемой поиска. Для обнаружения уязвимостей используются специализированные программные продукты, называемые сетевыми сканерами. Принцип работы сетевых сканеров заключается в следующем:

1. Подсистема поиска с установленным сетевым сканером подключается к сети.

2. В заданном диапазоне IP-адресов производится поиск доступных сетевых ресурсов, идентификация сетевых сервисов и первичный анализ их уязвимости.

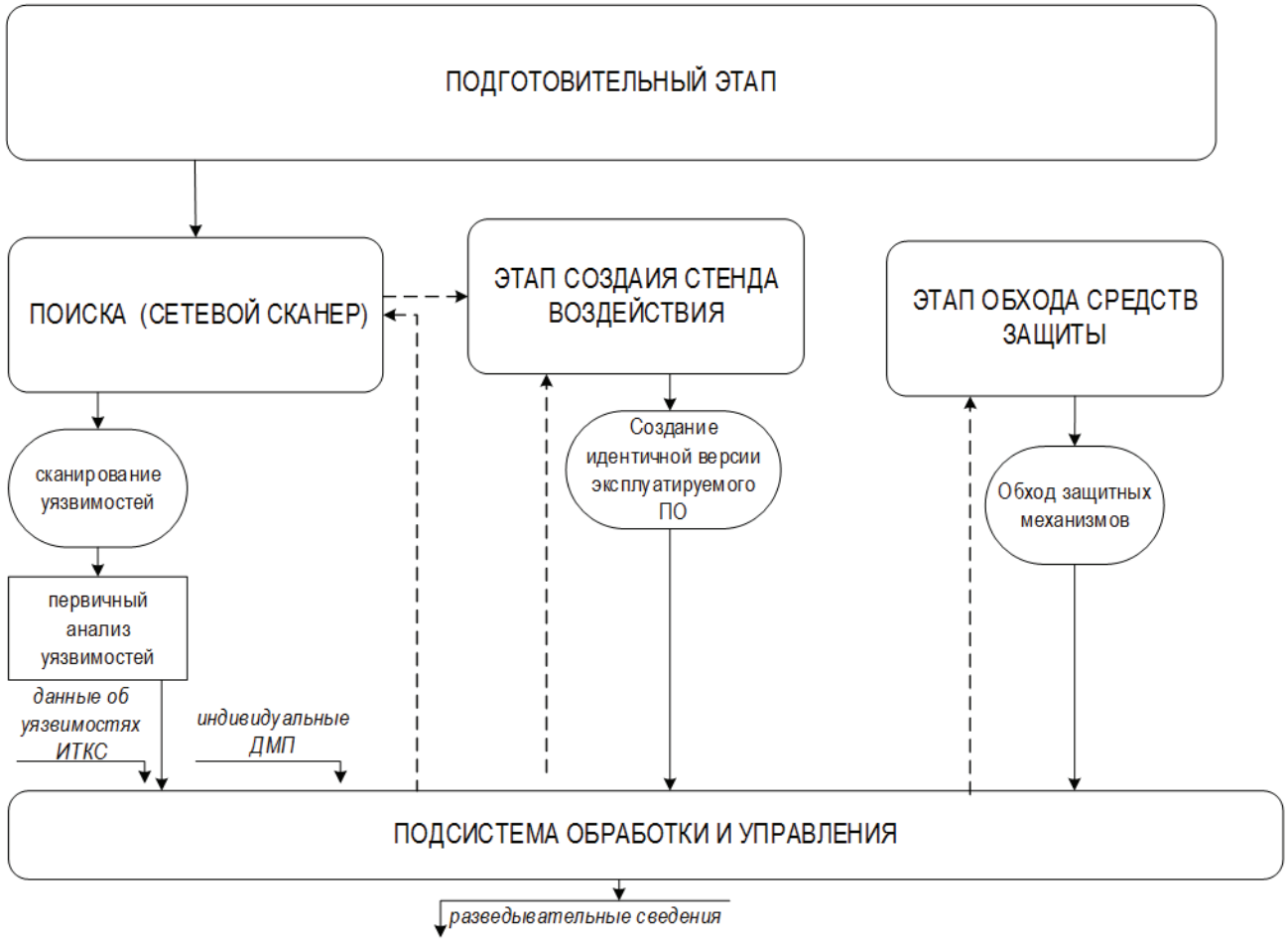


Рис. 1. Функциональная модель подготовительной функции ТКА

3. По результатам сканирования автоматически готовится отчет о составе сетевых ресурсов, состоянии защищенности каждого сетевого ресурса, обнаруженных уязвимостях в системе защиты и оценке возможности использования этих уязвимостей для проникновения в систему, который передаётся в подсистему обработки и управления.

Процесс сканирования можно представить в виде пошаговой процедуры:

1. Задание параметров сеанса сканирования.

2. Автоматическое обнаружение сетевых ресурсов;

3. Сбор и анализ данных, определение уязвимостей;

4. Представление результатов сканирования;

5. Автоматическая подготовка отчета.

Сканирование сетевых ресурсов, автоматическое обнаружение узлов и услуг позволяет собирать информацию обо всех сетевых устройствах, находящихся в исследуемой сети, таких как АРМ, почтовые серверы, межсетевые экраны, маршрутизаторы, серверы удаленного доступа и т.д. Эта функция позволяет составить полную карту работающих в сети активных устройств и активизированных сетевых услуг путём «опроса» сетевых устройств по соответствующим протоколам [7].

Сканер выполняет проверку всех IP-адресов и портов из заданного диапазона и таким образом строит карту сегмента сети. По созданной карте сегмента сети сканер начинает сбор данных по всем сетевым ресурсам. Подобное исследование сегмента сети значительно увеличивает сетевой трафик, что является одним из признаков проведения сканирования.

Затем анализирует собранную информацию с целью определения базовых параметров (типа операционной системы, включенных сетевых сервисов и т.п.) и потенциальных уязвимостей, обычно присутствующих в настройках ОС и сетевых служб. Сведения об уязвимостях заложены в базу данных сканера в виде правил, которые применяются для каждого конкретного узла из заданного диапазона. В данном случае сканер просто перебирает уязвимости и отмечает степень их потенциальной пригодности к использованию. Этот этап является активным и предполагает достаточно большое количество запросов, посылаемых по сети к каждому исследуемому узлу, но никаких деструктивных действий сканер не производит.

Результаты сканирования каждого узла сети представляются в виде отчёта, содержащего сведения об обнаруженных уязвимостях, типе операционной системы, перечне портов и соответствующих им функций.

Эффективность функционирования подсистемы поиска и технического анализа можно оценить вероятностью обнаружения уязвимостей по известным сценариям ($P_{\text{обн.}}$).

Данные поступают в подсистему обработки и управления, где определяется оперативно-тактическая принадлежность объектов разведки (объект вскрывается), а также производится управление функционированием всех подсистем.

Если по результатам обработки указанных данных, было выявлено, что сеть защищена средствами защиты, то реализуется подсистема создания стенда воздействия ТКА, в которой создается идентичная версия эксплуатируемого ПО, реализуются этапы проникновения в инфраструктуру сети ИТКС, в обход стандартных средств защиты с помощью скрытого внедрения.

Этот этап является главным переходом между пассивной и активной фазами проникновения в инфраструктуру сети ИТКС.

Результаты воздействия представляются в виде отчёта, содержащего сведения об реализации этапов проникновения в сеть. Эффективность функционирования подсистемы создания стенда воздействия можно оценить вероятностью создания ложной системы ($P_{\text{созд.}}$).

Далее осуществляются активные действия, с этой целью включается подсистемы обхода стандартных средств защиты ИТКС. Собранная информация уязвимостей в средствах защиты, позволяет обмануть либо обойти защитные механизмы, которые используют все привилегии легитимного процесса в своих целях, не обращая на себя внимание.

Результаты обхода средств защиты представляются в виде отчёта, содержащего сведенья об обходе защиты, закреплении во взломанной системе и сокрытии следов присутствия. Эффективность функционирования подсистемы обхода стандартных средств защиты ИТКС можно оценить вероятностью скрытия воздействия ($P_{\text{обход.}}$).

После обхода стандартных средств защиты повторно включается подсистема поиска (сетевое сканирование) с целью изучения работы топологии и с учётом структуры сети.

Результаты сканирования каждого узла сети представляются в виде отчёта, содержащего сведения об обнаруженных уязвимостях, типе операционной системы, перечне портов и соответствующих им функций. Эффективность функционирования подсистемы поиска и технического анализа можно оценить вероятностью обнаружения уязвимостей по известным сценариям ($P_{\text{обн.}}$).

Далее включаетсяразработка набора инструментов воздействия на ИТКС (рис. 2).

Реализуя следующие мероприятия:

1. Внедрение вредоносного кода, используя уязвимости в программном обеспечении с целью:

– создания вредоносного кода, который учитывает уязвимости системы;

– закрепления внутри зараженной системы, скрытой автозагрузки;

– обеспечения передачи команд;

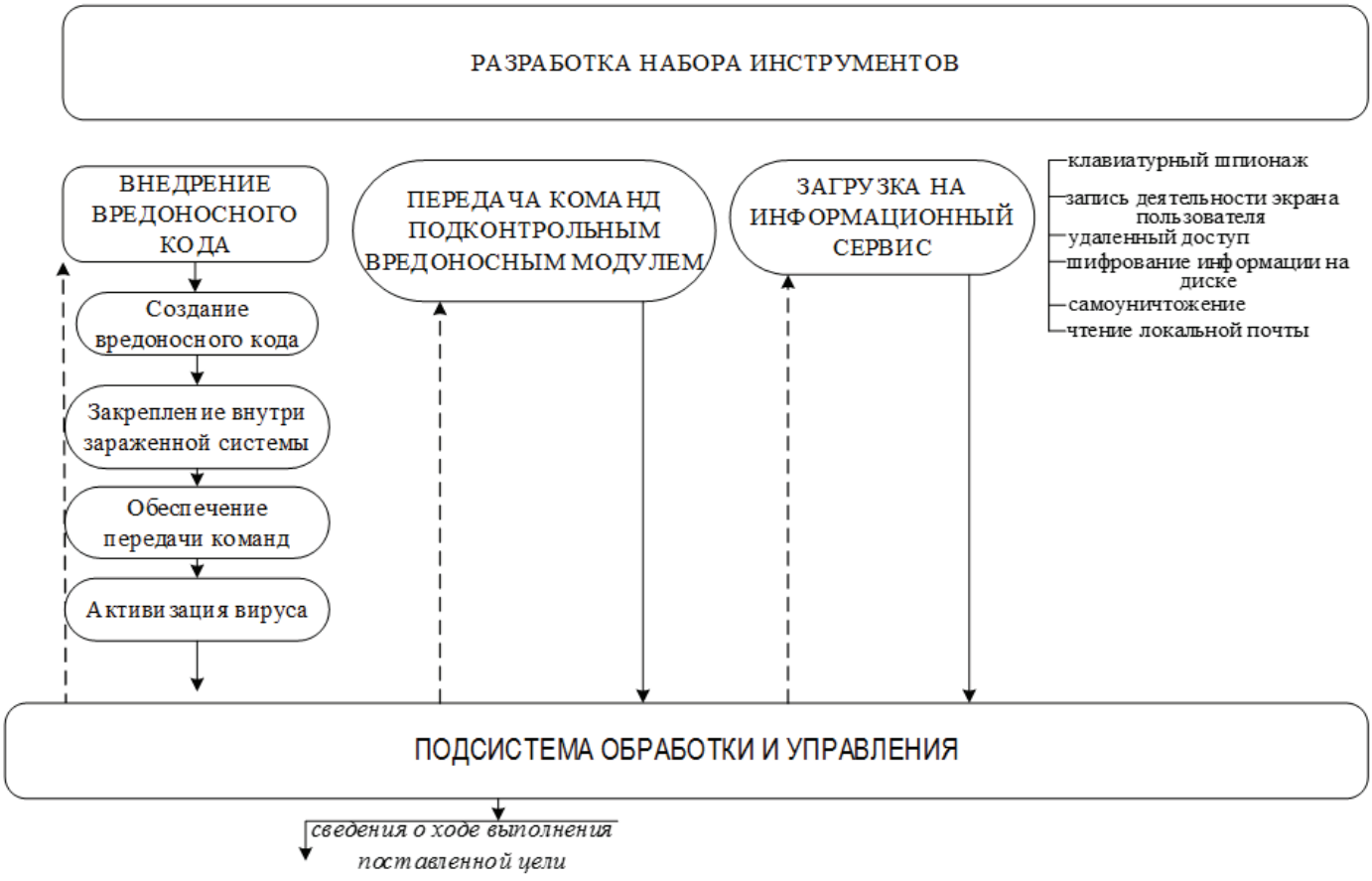


Рис. 2. Функциональная модель подготовительной функции ТКА

– внедрения в легитимный процесс для активизации вируса по шифрованному каналу, либо извлечение и запуск зашифрованной копии вируса с диска.

2. Обеспечение передачи команд подконтрольным вредоносным модулем, с которого собираются результаты работы.

3. Загрузка на инфицированный сервис основного вредоносного модуля ТКА, который может состоять из следующих подмодулей:

– клавиатурного шпионажа, который используется для контроля и записи (регистрации) каждого нажатия клавиш на компьютерной клавиатуре;

– записи деятельности экрана пользователя;

– удаленного доступа, который обеспечивает возможность доступа к файлам и их передачи;

– модуль распространения внутри инфраструктуры, для извлечения информации, срыва или создание помех критическим аспектам выполнения задач, программ или служб;

– шифрования информации на диске;

– очистка следов активности, самоуничтожение;

– чтение локальной почты;

– поиск информации на диске.

Результаты разработки набора инструментов представляется в виде отчёта, содержащего сведения об реализации внедрения вредоносного кода и загрузки вредоносного модуля [8]. Эффективность функционирования подсистемы разработки набора инструментов можно оценить вероятностью распределения средств воздействия ($P_{\text{р.н.и.}}$).

Далее осуществляется несанкционированный доступ (рис. 3). Он делится на следующие фазы:

– закрепления внутри инфраструктуры;

– распределение;

– пополнение;

– мониторинг и выбор метода достижения цели.

Закрепление внутри инфраструктуры, осуществляется гарантированным доступом в инфраструктуру ИТКС путем выполнения роли загрузчика, позволяющий загружать вредоносный модуль при включении АРМ и выгружать его при выключении или копировании системной папки загрузчика со следующими атрибутами: системные; скрытые; только для чтения [13–15]. Запуск осуществляется с помощью сервиса со схожим системным именем, отличающийся одной точкой.

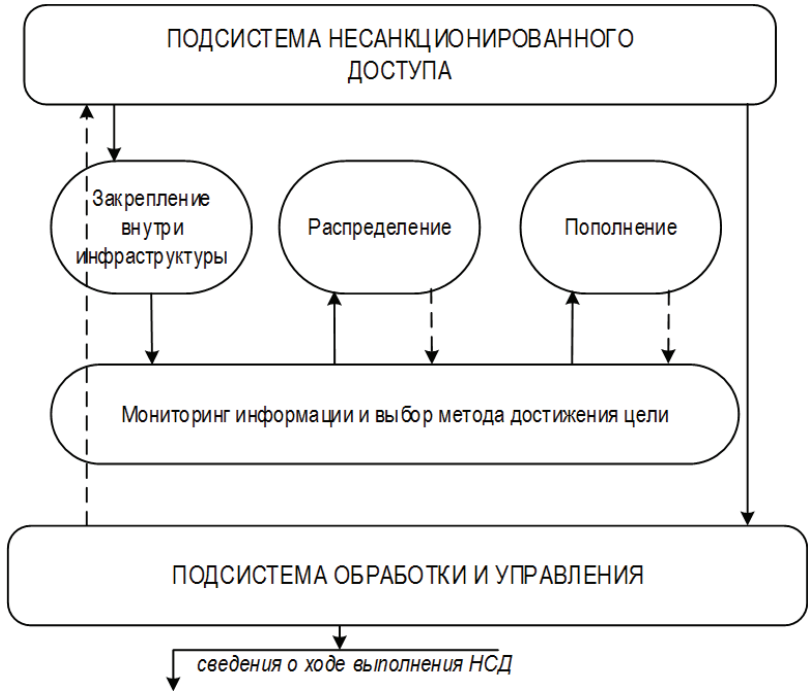


Рис. 3. Функциональная модель несанкционированного доступа ТКА

Результаты закрепления внутри инфраструктуры представляются в виде отчёта, содержащего сведенья гарантированного доступа в инфраструктуру. Эффективность функционирования подсистемы закрепления внутри инфраструктуры можно оценить вероятностью поражения и захвата модуля ($P_{з.в.и.}$).

Подсистема распределения, осуществляет запуск вредоносного модуля, путем подключения к выбранному АРМ удаленным RDP-клиентом, который используется для обеспечения удаленной работы пользователя с сервером.

Результаты распределения представляются в виде отчёта, содержащего сведенья заражения сети. Эффективность функционирования подсистемы распределения можно оценить вероятностью эффективности воздействия ($P_{расп}$).

В случае отсутствия определенной функции в арсенале, осуществляется этап пополнения, который автоматически обновляет модуль [9].

Завершающий этапом ТКА выполняет подсистема мониторинга и выбора метода достижения цели. Имея доступ в инфраструктуре АРМ, реализуется пассивные вредоносные действия, которое не оказывают непосредственное влияние на работу АРМ, но может нарушить ее политику безопасности. Основными вредоносными действиями является:

– хищения/удаления и/или искажения информации;
– внедрение вредоносных кодов;
– отказ в обслуживании;
– перенаправление трафика;
– техническая компьютерная разведка.

Результаты распределения представляются в виде отчёта о выполнении вредоносного действия. Эффективность функционирования подсистемы мониторинга и выбора метода достижения цели можно оценить вероятностью поражения ($P_{дост.}$).

На всех подсистемах осуществляется контроль по сокрытию следов, если присутствие опознано, на любом из подсистем, то выполняется чистка журнала событий. Как правило, большая часть активности протекает под административным доступом, не вызывая подозрения.

В случаи если в сети не используются средства защиты, либо они неправильно были настроены пользователем, то реализация ТКА после выполнения подсистемы поиска (сетевого сканирования) приступает сразу к подсистеме разработки набора инструментов воздействия на ИТКС.

После первой успешной реализации для уменьшения времени ТКА, сохраняется файл возврата, для дальнейшей реализации атак с подсистемы мониторинга и метода достижения цели [2].

По описанной выше модели была определена степень опасности ТКА, для этого была рассмотрена физическая основа этапов ТКА, особенности их воздействия, характер проявления на элементах ИТКС.

Анализ рассмотренной ТКА и способов её реализации (табл. 1) позволяет определить места проявления ТКА

Таблица 1

Способы реализации ТКА

Этапы реализации ТКА	Способы реализации	Область проявления
I. Поиск (сетевое сканирование)	1.1. Анализ сетевого трафика.	Канал связи
	1.2. Сканирование сети и её уязвимостей.	Коммутатор, Маршрутизатор, ПЭВМ, Серверы
	1.3. Сканирование протоколов передачи данных сети.	
II. Создание стенда воздействий	2.1. Виртуальный	
	2.2. Аналитический	
	2.3. Имитационный	
III. Обход стандартных средств защиты	3.1. Обфускация модулей (вирусных сигнатур) с целью маскировки от антивирусов	Коммутатор Маршрутизатор ПЭВМ
	3.2. Выявление уязвимостей испытуемой системы	
	3.3. Инжектирование процесса (пост-эксплуатация)	
	3.4. Эксплуатация системы	
	3.5. Внедрение вирусных сигнатур в систему	
IV. Разработка набора инструментов	4.1. Средства создания инструментов воздействия	Коммутатор, Маршрутизатор, ПЭВМ, Серверы
	4.2. Тело вируса Payload	ПЭВМ
V. Закрепление внутри инфраструктуры	5.1. Инструменты эксплуатации	Коммутатор, Маршрутизатор, ПЭВМ Серверы
VI. Мониторинг и выбор метода достижения цели	6.1. Хищение, удаление и/или искажение информации	ПЭВМ, Серверы
	6.2. Отказ в обслуживании	Коммутатор, Маршрутизатор, ПЭВМ Серверы
	6.3. Перенаправление трафика	Маршрутизатор, ПЭВМ, Серверы

в ИТКС. Для этого на основе метода анализа иерархии и метода максимального элемента [10–12], была спрогнозирована структура наиболее опасной ТКА, а также места ее проявления.

Используя полученные значения в качестве исходных данных, были определены показатели, характеризующие защищенность сети через ВВХ ТКА. Для этого первоначально была построена профильная модель ТКА, включающая следующие этапы:

– с вероятностью P_{I} осуществляется поиск (сетевое сканирование) выполняя сканирование сети и её уязвимостей за среднее время $t_{\text{поиск}}$ с функцией распределения $Q(t)$;

– с вероятностью P_{II} осуществляется, этап создания имитационного стенда воздействия за среднее время $t_{\text{с.с.в.}}$ с функцией распределения $Y(t)$;

– с вероятностью P_{III} осуществляется этап обхода стандартных средств защиты выполняя выявление уязвимостей испытуемой системы за среднее время $t_{\text{обход.}}$ с функцией распределения $U(t)$;

– с вероятностью P_{IV} осуществляется этап разработки набора инструментов выполняя создание инструментов воздействия за среднее время $t_{\text{р.н.и.}}$ с функцией распределения $R(t)$;

– с вероятностью P_{V} осуществляется этап закрепление внутри инфраструктуры с помощью инструмента экс-

плуатации Cracrle за среднее время $t_{з.в.и.}$ с функцией распределения $L(t)$;

– с вероятностью P_{VI} осуществляется этап распределения за среднее время $t_{расп}$ с функцией распределения $H(t)$;

– с вероятностью P_{VII} осуществляется этап пополнения за среднее время $t_{попол}$ с функцией распределения $J(t)$;

– с вероятностью P_{VIII} осуществляется этап мониторинга и выбора достижения цели выполняя хищение, удаление и/или искажение информации за среднее время $t_{дост.}$ с функцией распределения $V(t)$.

Описанный процесс представим в виде стохастической сети (рис. 4).

Используя правила преобразования профильных моделей по правилам топологического преобразования стохастических сетей, получены расчетные выражения для интегральной функции распределения вероятности и среднего времени реализации ТКА [5].

Результаты расчета представлены в виде зависимостей (рис. 5).

В качестве исходных данных используются следующие значения:

$t_{поиск}$ = 70 мин; P_I = 0,5…0,9;

$t_{с.с.в.}$ = 63 мин; P_{II} = 0,5…0,9;

$t_{обход.}$ = 73 мин; P_{III} = 0,5…0,9;

$t_{р.н.и.}$ = 53 мин; P_{IV} = 0,5…0,9;

$t_{з.в.и.}$ = 34 мин; P_V = 0,5…0,9;

$t_{расп}$ = 12 мин; P_{VI} = 0,5…0,9;

$t_{попол}$ = 8 мин; P_{VII} = 0,5…0,9;

$t_{дост.}$ = 5 мин; P_{VIII} = 0,5…0,9.

Учитывая физический смысл интегральной функции распределения оценку устойчивости сети можно определить из выражения:

$$K_И = 1 - F(t)$$

Настоящая статья предлагает новый подход к аналитическому моделированию таргетированных компьютерных атак, основанный на методе преобразования стохастических сетей. Сущность данного метода заключается в замене множества элементарных ветвей стохастической сети одной эквивалентной ветвью и последующим определением эквивалентной функции сети, а также начальных моментов и функции распределения случайного времени реализации компьютерной атаки . Проверка предложенного подхода была произведена для формирования эталонной модели таргетированной атаки, которые являются наиболее характерными и опасными для больших распределенных компьютерных сетей.

Разработанный метод аналитического моделирования атак положен в основу предложенной методики оценки устойчивости компьютерной сети в условиях таргетированных компьютерных атак. Применение в методике эталонных моделей атак и метода преобразования стохастических сетей позволяет определить вероятностно-временные характеристики таргетированной компьютерной атаки, которые являются исходными данными для методики.

Литература

1. *Коцыняк М.А., Иванов Д.А.* Обеспечение безопасности управления роботизированных систем от воздействия таргетированных кибернетических атак // Тезисы докладов XVI Всероссийская научная конференция «Нейрокомпьютеры и их применение» (Москва, 13 марта 2018 г.). Москва, 2018. С. 108-А.

2. *Гудков М.А., Лаута О.С., Иванов Д.А., Соловьев Д.В.* Применение методов искусственного интеллекта в задачах обеспечения информационной безопасности // Материалы IV Всероссийской научно-практической конференции «Современные информационные технологии. Теория и практика» (Череповец, 04 декабря 2017 г.). Череповецкий государственный университет, 2018. С. 162–166.

3. Лаута О.С., Кузнецов С.И., Клинцов И.А., Смыгин А.М. Методика оценки компьютерных угроз на ИТКС // Сборник трудов XXIII Международной научно-технической конференции «Радиолокация, навигация, связь» (Воронеж, 18–20 апреля 2017 г.). В 3-х томах. Воронеж: Вэлборн, 2017. С. 1200.

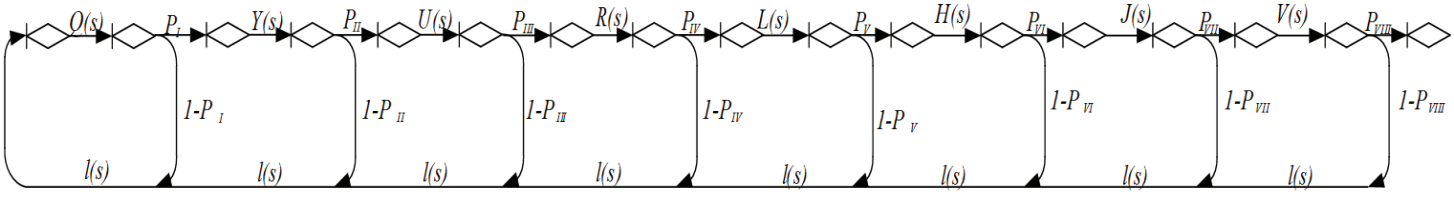
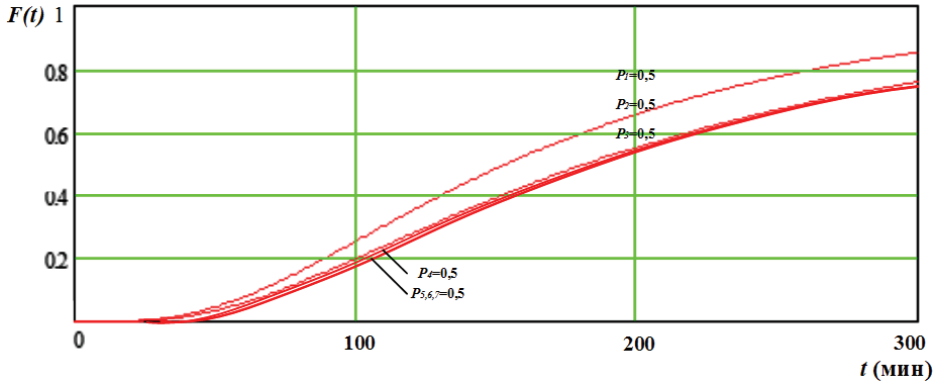
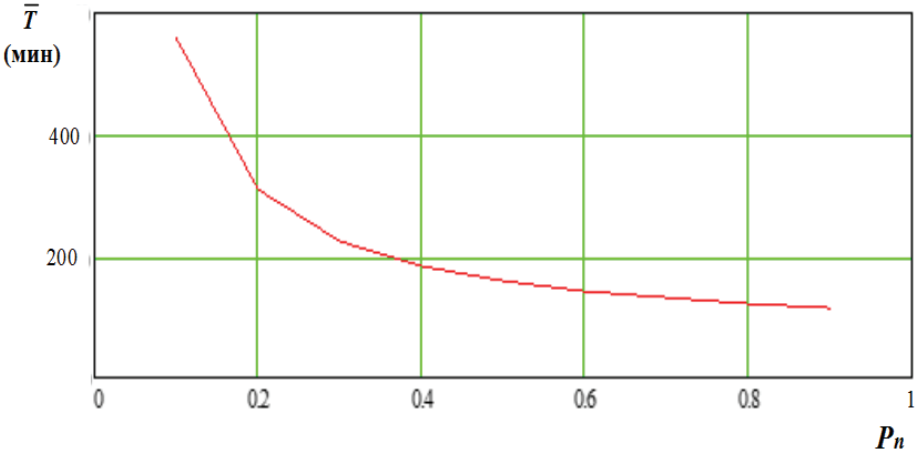


Рис. 4. Стохастическая сеть ТКА



а)



б)

Рис. 5. Вероятностно-временные характеристики реализации ТКА:
а) зависимость интегральной функции распределения вероятности от времени реализации этапов ТКА
б) зависимость среднего времени реализации ТКА от вероятности реализации каждого ее этапа

4. *Коцыняк М.А., Дементьев В.Е., Тесля С.П., Лаута О.С.* Методика прогнозирования протокольных воздействий на роботизированные системы // Сборник трудов юбилейной X Санкт-Петербургской межрегиональной конференции «Региональная информатика и информационная безопасность» (ISRR-2017) (Санкт-Петербург, 01–03 ноября 2017 г.). СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 105–107.

5. *Коцыняк М.А., Иванов Д.А., Лаута О.С., Нечепуренко А.П., Муртазин И.Р.* Методика прогнозирования воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Сборник трудов юбилейной X Санкт-Петербургской межрегиональной конференции «Региональная информатика и информационная безопасность» (ISRR-2017) (Санкт-Петербург, 01–03 ноября 2017 г.). СПб.: Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления, 2017. С. 109–111.

6. *Иванов Д.А., Коцыняк М.А., Лаута О.С., Мур-тазин И.Р.* Методика кибернетической устойчивости в условиях воздействия таргетированных кибернетических атак // Сборник научных статей VII Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2018) (Санкт-Петербург, 28 февраля – 01 марта 2018 г.). В 4-х томах / Под редакцией С.В. Бачевского. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. С. 343–346.

7. *Карганов В.В., Драчев В.О., Левченко Г.Н.* Формирование модели предметной области для информационной системы // Труды десятой общероссийской научно-практической конференции «Инновационные технологии и технические средства специального назначения» (Санкт-Петербург, 15–16 ноября 2018 г.). СПб.: Балтийский государственный технический университет «Военмех», 2018. С. 264–268.

8. *Карганов В.В., Липатников В.А., Литвинов А.А.* Распознавание вторжений и анализ динамики действий нарушителя при управлении информационно-вычислительной сетью // Материалы конференций ГНИИ «Нацразвитие» (Санкт-Петербург, 28–31 января 2018 г.). СПб., 2018. С. 28–36.

9. *Берзин Е.А.* Оптимальное распределение ресурсов и элементы синтеза систем. М.: Советское радио, 1974. 304 с.

10. *Luvanda A., Kimani S., Kimwele M.* Identifying Threats Associated With Man-In-The Middle Attacks during Communications between a Mobile Device and the Back End Server in Mobile Banking Applications // IOSR Journal of Computer Engineering (IOSR-JCI). 2014. No. 12(2). Pp. 35–42.

11. *Kelly F., Yudovina E.* Stochastic Networks. Cam-bridge: Cambridge University Press, 2014. 222 p.

12. *Saenko I., Lauta O., Kotenko I.* Analytical modeling of mobile banking attacks based on a stochastic network conversion technique // International Symposium on Mobile Internet Security MobiSec 2016: Mobile Internet Security. CCIS, volume 797. Pp 107–117.

13. OPNET Technologies, Inc. URL: http://www.opnet.com/ (дата обращения 07.10.2018)

14. A*huja S.P.* COMNET III: A Network Simulation Laboratory Environment For A Course In Communications Networks // 28th Annual Frontiers in Education Conference (FIE ‘98). 1998. Vol. 3. Pp. 1085–1088.

15. *Kotenko A., Chechulin A.* Cyber Attack Modeling and Impact Assessment Framework // Proc. of the 5th IEEE International Conference on Cyber Conflict (CyCon). 2013. Pp. 1–24.

METHODOLOGY FOR ASSESSMENT OF NETWORK STABILITY IN THE CONDITIONS OF TARGETED CYBERNETIC ATTACK

MIKHAIL A. KOTSYNYAK,
Russia, st. Petersburg, koc-1942@mail.ru

OLEG S. LAUTA,
Russia, St. Petersburg, laos-82@yandex.ru

DENIS A. IVANOV,
Russia, St. Petersburg, prosto_deniss@mail.ru

KEYWORDS: attack modeling; computer network security; stochastic networks; Laplace transform.

ABSTRACT

Effective and reliable protection of a computer network is impossible without a preliminary analysis of possible threats to its security, among which the most powerful are targeted computer attacks. Targeted computer attacks and the ability to counteract their implementation are key factors determining the stability of computer networks. Assessing the stability of a computer network under the conditions of the targeted computer attacks, which is understood as its ability to withstand various types of passive and active attacks and maintain indicators of its functioning under the impact of these attacks, is quite an important and difficult task. Analytical modeling of targeted computer attacks helps in many ways to effectively solve this problem. This work proposes to apply the method of transformation of stochastic networks for analytical modeling of various types of targeted computer attacks and use the simulation results to solve the problem of assessing the stability of a computer network. The essence of the method lies in the fact that it is not the system that is investigated, but the target process that it implements. This complex process is decomposed into elementary processes, each of which can be characterized by the distribution function of the process execution time, the probability density, the probability or the average and variance of the execution time. This approach is distinguished by higher accuracy and stability of the solutions obtained. He has worked well for modeling multistep stochastic processes of various nature. The calculation of the network stability indicators under the conditions of the targeted cybernetic attacks was carried out through the probability-time characteristics. For this, the physical bases for the implementation of targeted computer attacks are developed, the profile models of the targeted computer attacks exposure stages are developed, and the transformation of stochastic networks method is used to calculate the probability-time characteristics of all the targeted computer attacks stages. The theoretical contribution of the work lies in the further development of methods of analytical modeling of computer attacks and in their application to assess sustainability as a very important feature of a computer network. The novelty of the results obtained is determined using the method of transformation of stochastic networks for analytical modeling of computer attacks.

REFERENCES

1 Kotsynyak M.A., Ivanov D.A. Obespechenie bezopasnosti upravleniya robotizirovannykh sistem ot vozdeystviya targetirovannykh kiberneticheskikh atak [Ensuring the security of control of robotic systems from the effects of targeted cybernetic attacks]. *Tezisy dokladov XVI Vserossiyskaya nauchnaya konferentsiya "Neyrokomp'yutery i ikh primenenie"* [Abstracts XVI all-Russian scientific conference "Neurocomputers and their application" (Moscow, March 13, 2018)]. 2018. P. 108-A. (In Russian)

2. Gudkov M.A., Lauta OS, Ivanov D.A., Soloviev D.V.Primenenie metodov iskusstvennogo intellekta v zadachakh obespecheniya informatsionnoy bezopasnosti [The use of artificial intelligence methods in the tasks of ensuring information security]. *Materialy IV Vserossiyskoy nauchno-prakticheskoy konferentsii "Sovremennye informatsionnye tekhnologii. Teoriya i praktika"* [Materials of the IV all-Russian scientific-practical conference " Modern information technologies. Theory and practice" (Cherepovets, December 04, 2017)]. Cherepovets, 2018. Pp. 162–166. (In Russian)

3. Lauta O.S., Kuznetsov S.I., Klinshov I.A., Smygin A.M. Metodika otsenki komp'yuternykh ugroz na ITKS [Methods of assessing computer threats to ITX]. *Sbornik trudov XXIII Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii "Radiolokatsiya, navigatsiya, svyaz'"* [Proceedings of the XXIII International scientific and technical conference " Radar, navigation, communication "(Voronezh, April 18–20, 2017)]. In 3 volumes. Voronezh: Вэлборн, 2017. P. 1200. (In Russian)

4. Kotsynyak M.A., Dementiev V.E., Teslya S.P., Lauta O.S.Metodika prognozirovaniya protokol'nykh vozdeystviy na robotizirovannye sistemy [Methods of predicting protocol effects on robotic systems]. *Procc. of the Anniversary X St. Petersburg Interregional Conference "Information security of russian regions (ISRR-2017)"* (St. Petersburg, 1–3 November 2017). St. Petersburg, 2017. Pp. 105–107. (In Russian)

5. Kotsynyak M.A., Ivanov D.A., Lauta O.S., Nechepurenko A.P., Murtazin I.R. Metodika prognozirovaniya vozdeystviya targetirovannoy kiberneticheskoy ataki na informatsionno-telekommunikatsionnuyu set' [Methods of predicting the impact of a targeted cyber attack on an information and telecommunication network]. *Procc. of the Anniversary X St. Petersburg Interregional Conference "Information security of russian regions (ISRR-2017)"* (St. Petersburg, 1–3 November 2017). St. Petersburg, 2017. Pp. 109–111. (In Russian)

6. Ivanov D.A., Kotsinyak M.A., Lauta O.S., Murtazin I.R. Metodika kiberneticheskoy ustoychivosti v usloviyakh vozdeystviya targetirovannykh kiberneticheskikh atak [Methods of cybernetic sustainability under the conditions of impact of targeted cybernetic attacks]. *Sbornik nauchnykh statey VII Mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii "Aktual'nye problemy infotelekommunikatsiy v nauke i obrazovanii" (APINO 2018)* [Collection of scientific articles VII International scientific-technical and scientific-methodical conference "Actual problems of infotelecommunications in science and education" (APINO 2018) (St. Petersburg, February 28-March 01, 2018)]. In 4 vol. St. Petersburg, 2018. Pp. 343–346. (In Russian)

7. Karganov V.V., Drachev V.O., Levchenko G.N. Formirovanie modeli predmetnoy oblasti dlya informatsionnoy sistemy [Formation of a domain model for an information system]. *Trudy desyatoy obshcherossiyskoy nauchno-prakticheskoy konferentsii "Innovatsionnye tekhnologii i tekhnicheskie sredstva spetsial'nogo naznacheniya"* [Proceedings of the tenth all-Russian scientific and practical conference "Innovative technologies and technical means of special purpose" (St. Petersburg, November 15–16, 2018)]. St. Petersburg, 2018. Pp. 264–268. (In Russian)

8. Karganov V.V., Lipatnikov V.A., Litvinov A.A. Detection of intrusions and analysis of the dynamics of the offender's actions in managing the information and computing network. *Materialy konferentsiy Gumanitarnogo natsional'nogo issledovatel'skogo instituta "Natsrazvitie"* [Proceedings of the conferences of the Humanitarian national research Institute "national Development" (St. Petersburg, January 28–31, 2018)]. St. Petersburg, 2018. Pp. 28–36. (In Russian)

9. Berzin E.A. *Optimal'noe raspredelenie resursov i elementy sinteza sistem* [Optimal resource allocation and elements of system synthesis]. Moscow: Soviet Radio, 1974. 304 p. (In Russian)

10. Luvanda A., Kimani S., M. Kimwele M. Identifying Threats Associated With Man-In-The Middle Attacks during Communications between a Mobile Device and the Back End Server in Mobile Banking Applications. *IOSR Journal of Computer Engineering (IOSR-JCI).* 2014. No. 12(2). Pp. 35–42.

11. Kelly F., Yudovina E. *Stochastic Networks*. Cambridge: Cambridge University Press, 2014. 222 p.

12. *Saenko I., Lauta O., Kotenko I.* Analytical modeling of mobile banking attacks based on a stochastic network conversion technique. International Symposium on Mobile Internet Security MobiSec 2016: Mobile Internet Security. CCIS, 2016. Vol. 797. Pp 107–117.

13. OPNET Technologies, Inc. URL: http://www.opnet.com/ (date of access 07.10.2018)

14. Ahuja S.P. COMNET III: A Network Simulation Laboratory Environment For A Course In Communications Networks. *28th Annual Frontiers in Education Conference (FIE '98).* 1998. Vol. 3. Pp. 1085–1088.

15. Kotenko A., Chechulin A. Cyber Attack Modeling and Impact Assessment Framework. *Proc. of the 5th IEEE International Conference on Cyber Conflict (CyCon).* 2013. Pp. 1–24.

INFORMATION ABOUT AUTHORS:

Kotsynyak M. A., PhD, Full Professor, Professor of the Military Academy of Communications. Marshal of the Soviet Union S.M. Budennogo;

Lauta O. S., PhD, Teacher of the Department of the Military Academy of Communications. Marshal of the Soviet Union S.M. Budennogo;

Ivanov D. A., Postgraduate student of the Military Academy of Communications. Marshal of the Soviet Union S.M. Budennogo.

For citation: : Kotsynyak M. A., LautaO. S., Ivanov D. A. Methodology for assessment of network stability in the conditions of targeted cybernetic attack. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 76–85. doi: 10.24411/2409-5419-2018-10189 (In Russian)

doi: 10.24411/2409-5419-2018-10190

ОБОСНОВАНИЕ АРХИТЕКТУРЫ СВЕРТОЧНОЙ НЕЙРОННОЙ СЕТИ ДЛЯ АВТОНОМНОГО РАСПОЗНАВАНИЯ ОБЪЕКТОВ НА ИЗОБРАЖЕНИЯХ БОРТОВОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМОЙ

ХОМОНЕНКО
Анатолий Дмитриевич[1]

ЯКОВЛЕВ
Евгений Леонидович[2]

АННОТАЦИЯ

Предлагается подход к обоснованию архитектуры сверточной нейронной сети, обеспечивающий улучшение характеристик по числу весовых коэффициентов, соединений при сохранении точности распознавания объектов на изображениях. Обучение сверточной нейронной сети с выбранной архитектурой реализуется на Земле. После обучения нейронная сеть используется в бортовых вычислительных системах для автономного распознавания объектов на изображениях. Проводится анализ особенностей построения сверточной нейронной сети для распознавания объектов на изображениях, и на его основе формулируются ограничения и правила разработки новых сверточных нейронных сетей. Сформулирована постановка комбинаторной задачи оптимизации, предлагается эвристический алгоритм для решения этой задачи на основе правил компоновки и отсечения неперспективных конфигураций сверточной нейронной сети. Для тестовых наборов данных Planetsnet и MNIST приведены результаты компьютерных экспериментов и выполнено сравнение с существующими архитектурами сверточной нейронной сети по числу весовых коэффициентов, соединений и точности в % ошибок на тестовом множестве. Показано, что предложенный алгоритм позволяет выбрать вариант архитектуры сверточной нейронной сети с меньшим числом весовых коэффициентов и соединений при практически той же точности в % ошибок решения задачи распознавания объектов на изображении.

КЛЮЧЕВЫЕ СЛОВА: сверточная нейронная сеть; автономное распознавание объектов на изображениях; бортовая вычислительная система.

Сведения об авторах:

[1]д.т.н., профессор, заведующий кафедрой информационные и вычислительные системы Петербургского государственного университета путей сообщения Императора Александра I, г. Санкт-Петербург, Россия, khomonenko@pgups.ru

[2]адъюнкт Военно-космической академии имени А.Ф.Можайского г. Санкт-Петербург, Россия, evgen-1932@yandex.ru

Для цитирования: *Хомоненко А.Д., Яковлев Е.Л.* Обоснование архитектуры сверточной нейронной сети для автономного распознавания объектов на изображениях бортовой вычислительной системой // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 86–93. doi: 10.24411/2409-5419-2018-10190

Введение

Задачи автономного распознавания объектов на изображениях с помощью бортовых вычислительных систем летательных аппаратов имеют большую практическую значимость, В частности, задачи распознавания объектов требуется решать при дистанционном зондировании Земли с помощью авиации, космических средств и беспилотных летательных аппаратов (БЛА). Подавляющее большинство современных БЛА управляются человеком-оператором с помощью информационных каналов, самые «продвинутые» системы управления БЛА поддерживают режимы полета по заданным точкам, используя информацию от глобальных навигационных спутниковых систем.

Развитие быстродействующей вычислительной техники, совершенствование оптико-электронных датчиков определяет целесообразность исследования вопросов автономного анализа изображений на борту БЛА, с возможностью распознавания заранее определенных объектов, с дальнейшим использованием полученной информации для решения задач управления.

Решению задач распознавания изображений посвящено большое число публикаций, однако до сих пор эта проблема не решена полностью. Это связано с большой информационной емкостью и априорной неопределенностью, присущей изображениям, а также с большой изменчивостью изображений за счет изменение ракурса или освещения, что приводит к изменению значений одновременно во всех элементах изображения. В качестве наиболее эффективных методов следует указать:

– методы, основанные на шаблонах [1];
– методы с использованием контурных моделей [2–3];
– метод Виолы-Джонса и его комбинации [4–5];
– статистические методы (инварианты моментов) [6–7];
– нейросетевые методы [8].

Основной мировой тренд в области обнаружения и распознавания изображений заключается в применении сверточных нейронных сетей (СНС). Главным преимуществом такого подхода в сравнении с признаковым описанием, реализуемым первыми четырьмя методами в указанном списке, является то, что алгоритм по сути сам выделяет информативные признаки.

Для создания системы автономного распознавания объектов на изображениях бортовой вычислительной системой (на основе данных, получаемых с помощью оптических датчиков) предлагается использовать базу данных из СНС, заранее обученных на Земле. После обучения СНС используются для обработки входного потока изображений на борту летательного аппарата.

Проведенные эксперименты показали, что изменения высоты полета, ракурса съемки приводят к сильному ухудшению результативности распознавания, появляется необходимость адаптации изображений, получаемых оптическими датчиками, к разрешению входных окон обученных СНС. При уменьшении пространственного пиксельного разрешения изображения для сетей для более высоких высот такой подход реализуется успешно. Наоборот, при увеличении разрешения изображений различными методами распознавание объектов происходит неэффективно.

Для каждого конкретного распознаваемого класса объектов целесообразно эмпирически подобрать архитектуру СНС, причем объем вычислений должен не превышать возможности вычислительных устройств на борту БЛА. Такой подход значительно увеличивает время построения классификатора и/или внесения в него изменений. Из отмеченного следует целесообразность обоснования архитектуры СНС, оптимальной или близкой к оптимальной по вероятности распознавания при ограниченной производительности бортовой вычислительной системы.

1. Основные особенности построения СНС для задач распознавания объектов

Рассмотрим особенности эволюции современных сверточных сетей на примерах LeNet-5, AlexNet, VGG16, GoogLeNet, ResNet — перечисленные СНС в разное время становились лидерами в решении задач распознавания изображений.

Прежде всего рассмотрим обобщенную архитектуру СНС (LeNet-5) [9], использовавшуюся для распознавания рукописных цифр MNIST [10], являющуюся классическим вариантом архитектуры СНС (рис. 1). Сводные данные по этой архитектуре приведены в табл. 1.

На основе анализа архитектуры LeNet-5 можно отметить следующие ее особенности:

- в составе нейронной сети имеет место чередование слоев сверток (фильтров) и слоев субдискредитации;
- перед выходным (классифицирующим) слоем используются полносвязные слои;
- основное количество весовых коэффициентов приходится на полносвязные слои;
- порядок числа связей сохраняется и уменьшается от входа к выходу.

Особенностью архитектуры сети AlexNet [11] (рис. 2) является использование фильтров 11x11, 5x5 и 3x3. В качестве функции активации здесь впервые использовалась линейная функция ReLU. Сеть AlexNet разработана для тестового набора данных конкурса ImageNet и одержала победу в номинации распознавания рукописных цифр.

В архитектуре VGG16 [10] (рис. 3) использовались фильтры размерностью 3×3.

В СНС GoogLeNet [12], ResNet [13], используются типовые модули, последовательный набор которых определяет конфигурацию сети. Такие модули являются полноценными, но маленькими сверточными сетями, из которых строятся очень глубокие сети — до нескольких сотен слоев,

Таблица 1

Сводные данные по архитектуре СНС LeNet-5

Слои, №	Размер фильтра	∑ нейронов	Смещение	Выход слоя	Веса	Соединения
1	5x5	6	1	6@28x28	5*5*1*6+6=156	28*28*156=122304
2	2x2		2	6@14x14	12	14*14*30=5880
3	5x5	16	1	16@10x10	5*5*6*10=1516	10*10*1516=151600
4	2x2		2	16@5x5	32	5*5*80=2000
5	полносвязный	120		120	(400*120)+120=48120	48000
6	полносвязный	84		84	120*84+84=10164	10080
7	полносвязный	10		10	84*10+10=850	840

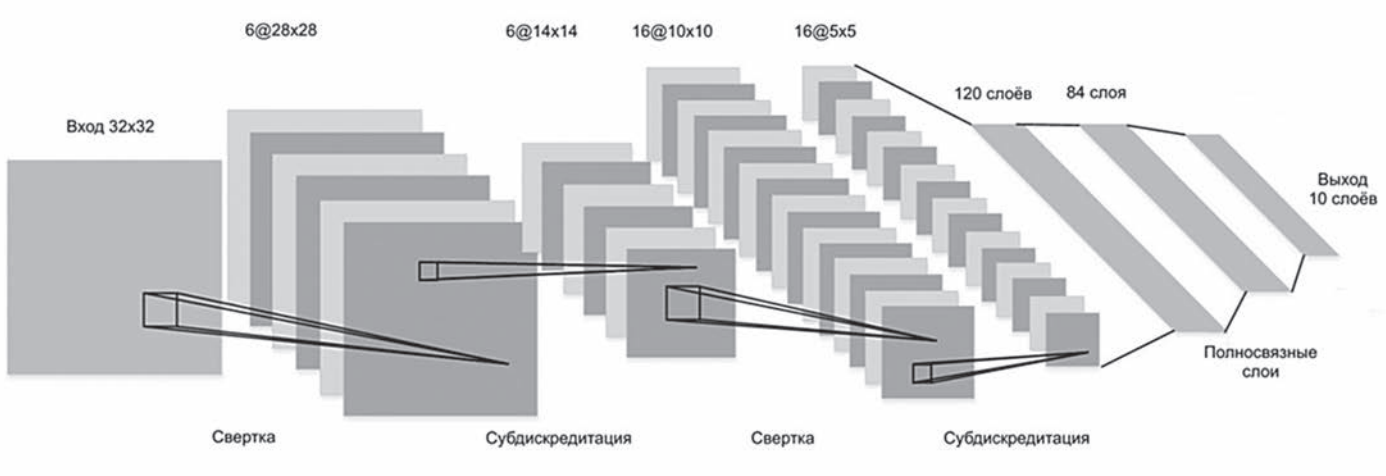


Рис. 1. Архитектура СНС LeNet-5

получает как бы маленькая вложенная сеть в большую. Название Inception (Начало) (рис. 4) отражает не только «глубину» из фильма «Inception», но и развитую там идею «вложенной» архитектуры: сон внутри сна внутри сна ….

Название Residual (остаточный), в свою очередь, по существу означает, что в блоке Residual (рис. 5) слой из нейронов можно обойти. Для этого есть специальная связь между выходом предыдущего слоя X и следующего слоя $Y = F(X)+X$, которая идет напрямую, а не через вычисляющий что-то слой.

Такая связь необходима для обучения сети — градиент во время обратного распространения сможет проходить через такой блок беспрепятственно, что решает проблему затухающих градиентов.

Анализ основных конфигураций СНС позволяет выделить основные особенности построения СНС:

1) вход и выход каждого элемента свертки связаны соотношениями:

$$y_{i,j}^{l} = h\left(\sum_{-d\le a,b\le d} W_{a,b} x_{i+a,j+b}^{l}\right) + C_{i,j}^{l},$$

где $y_{i,j}^{l}$ — выход свертки на уровне l, $x_{i,j}^{l}$ — вход, h — функция активации, $C_{i,j}^{l}$ — смещение, d — размер окна свертки;

2) при прохождении информации в целом по слоям сохраняется порядок числа соединений (кроме первого и последнего);

3) полносвязные слои обладают очень большим количеством параметров, их допустимо использовать только в выходном слое;

4) субдискредитация уменьшает количество соединений, элементы субдискредитации связаны соотношениями:

$$x_{i,j}^{l+1} = \max_{-d\le a\le d,-d\le b\le d} y_{i+a,j+b}^{l},$$

где d — размер окна субдискредитации;

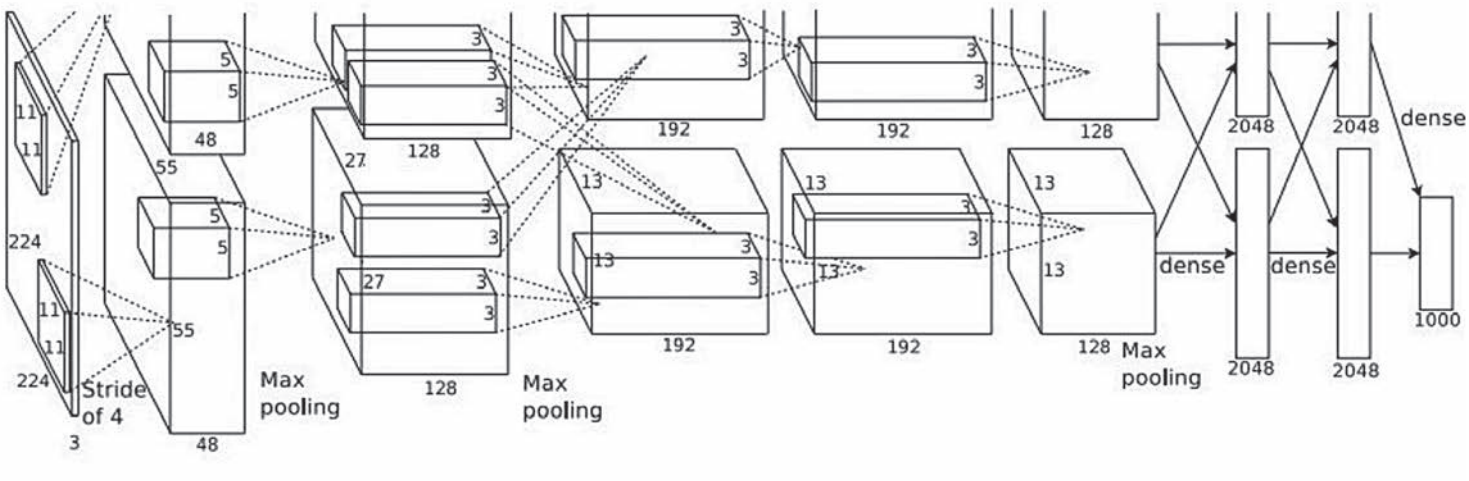


Рис. 2. Архитектура CHC AlexNet

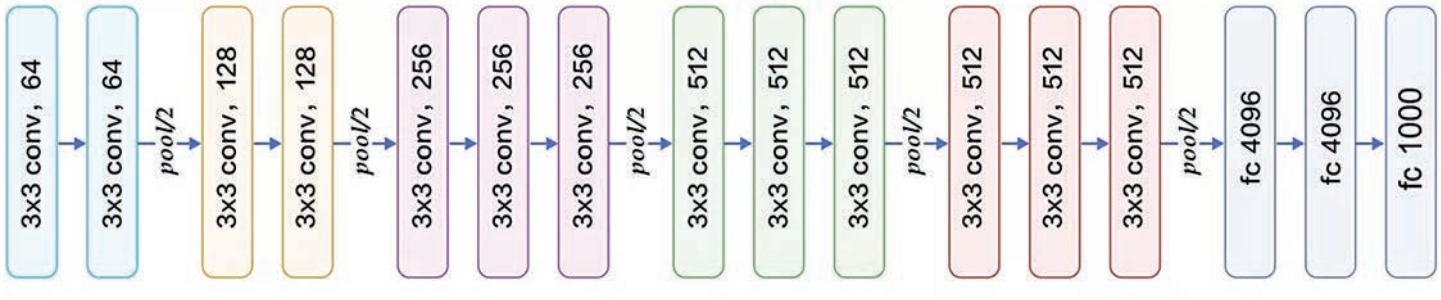


Рис. 3. Архитектура CHC VGG16

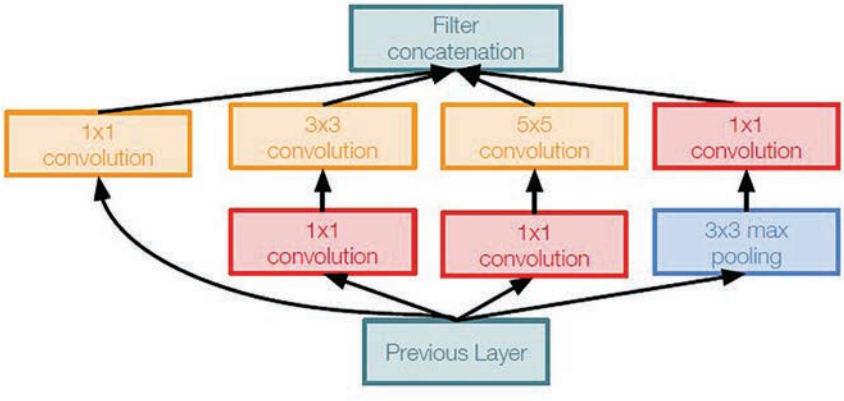


Рис. 4. Схема модуля Inception

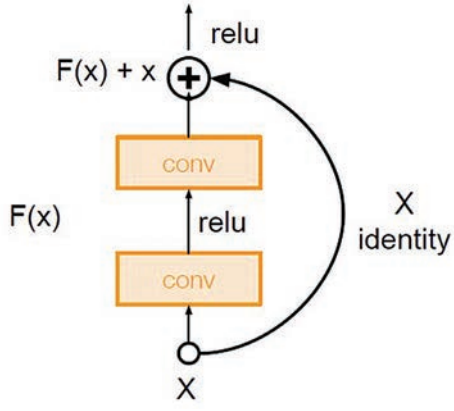


Рис. 5. Схема модуля Residual

5) использование фильтров меньшего размера 1×1, 3×3, а также модулей на их основе, ведет к уменьшению количества весовых коэффициентов, но увеличивает глубину сети, что приводит к трудностям при обучении;

6) использование фильтров большего размера 5×5, 7×7, 9×9, 11×11 ведет к увеличению числа весовых коэффициентов, но уменьшает глубину сети, что упрощает обучение;

При компоновке архитектуры предлагается использовать первые три правила, как ограничения, а ранжируя 4, 5, 6 правила в различном порядке — проводить поиск оптимальной конфигурации.

В ряде работ ставилась задача синтеза архитектуры нейронной сети [14–15] для прогнозирования параметров технического состояния и решения различных оптимизационных задач. В работе [16] предлагается подход на основе генетического алгоритма, но, несмотря на достижения в решении задач обучения нейронных сетей с помощью графических ускорителей, такой подход не позволяет найти требуемую архитектуру за приемлемое время.

2. Постановка задачи выбора конфигурации СНС

Дано:

– обучающая база: набор изображений $X=<m, n, ch>$ и соответствующие им классы $Y = \{y_i \mid i=1,..., r\}$, где r — число классов изображений;

– множество допустимых типов структурных элементов СНС $A = \{a_i \mid i=1,\ldots, n\}$, где n — число типов, в качестве элементов рассматриваются отдельные нейроны и базовые построения на основе нейронов в виде модулей Inception и Residual;

– $\gamma^5,\ s \in [1:3]$ — правила компоновки;

– модель распознавания $\hat{F}(A^{\text{СНС}})$: $X \to Y$, где $A^{\text{СНС}}$ — конфигурация структуры сверточной нейронной сети, задаваемая как состав элементов, матрица связей, количество связей будем считать равным количеству операций, необходимых для реализации $\hat{F}$;

– процессы задания начальных весовых коэффициентов и смещений, обучения конфигураций СНС происходят одинаково;

Ограничения:

– $\gamma^{\beta}, \beta \in [1:3]$ — ограничения на компоновку;

– Q — вычислительная трудоемкость, представленная количеством операций, необходимых на реализацию $\hat{F}(A^{\text{СНС}})$;

– M — используемая память, необходимая на реализацию $\hat{F}(A^{\text{СНС}})$.

Требуется:

Из множества $A^{\text{СНС}}$ альтернативных конфигураций СНС найти конфигурацию $A^{*\text{СНС}}$, обеспечивающую максимальный ожидаемый целевой эффект $\hat{F}$:

$$A^{*\text{СНС}} = \arg\max[\hat{F}(A^{\text{СНС}})].$$

Постановка задачи компоновки, в общем виде, похожа на классическую задачу о многомерном рюкзаке, однако в исходных данных отсутствует ценность каждого элемента из множества A.

Для решения такой задачи невозможно использовать классические методы дискретного нелинейного программирования, так как целевой функционал в данном случае стохастический (вероятность распознавания объектов из тестового множества), и его определение (обучение СНС) занимает значительное время. Нами предлагается использовать алгоритм направленно-случайного поиска, подобный эвристическому алгоритму, описанному в [17].

3. Алгоритм выбора конфигурации СНС

Перед реализацией алгоритма необходимо ввести понятие частичного разбиения, в качестве которого будем понимать совокупность слоев СНС $Z = \{Z_1,\ldots, Z_l\}$, где l — количество слоев СНС, задается экспертным путем. Основной идеей алгоритма является перебор комбинаторного множества конфигураций, ограниченных заданными ограничениями и правилами компоновки. Для уменьшения пространства перебора, по аналогии с методом ветвей и границ, для отсечения неперспективных альтернатив, будем использовать следующее правило:

Если из конфигурации СНС $Z^1 = \{Z_1^1,\ldots, Z_l^1\}$ при обучении которой достигнута точность (погрешность) P^1, получается конфигурация $Z^2 = \{Z_1^2,\ldots, Z_l^2\}$ путем изменения в одном произвольном слое $Z_e^1 = k_e^1 a_i$ элемента a_i на другой элемент a_{i+1} $Z_e^2 = k_e^2 a_{i+1}$, где $e \in [1,\ldots, l]$, k_e — число элементов в слое, причем $P^2 < P^1$. Тогда для конфигурации СНС Z^3 с $Z_e^3 = (k_e^2 + 1)a_{i+1}$, погрешность будет еще ниже $P^3 < P^2 < P^1$ и обучать дальше эту ветвь не надо.

Алгоритм компоновки конфигурации СНС предлагается в следующем виде:

1. В зависимости от обучающей базы задаются входной и выходной векторы нейронной сети они будут соответственно входным и выходным слоями искомой архитектуры:

– $x_{i,j}^1 = m * n * ch$;

– $y_{i,j}^l = r$.

2. Задаются произвольное число слоев l и счетчик компоновок $j = 1$. Определяется множество $A^{\text{СНС}}$.

3. $Q^* = 0$, $M^* = 0$, Z, $Z_1,\ldots, Z_l = \varnothing$, $j = j + 1$, $A^{\text{СНС}} = \varnothing$ — множество неперспективных архитектур.

4. $n = 1$ — счетчик слоев.

5. $k = 1$ — счетчик элементов в слое.

6. Проверка условия $n < l$, если выполняется, то переход на шаг 7, иначе переход на шаг 13.

7. В качестве правила выбора кандидата a_i из множества элементов A назначаются последовательно γ^5.

Таблица 2

Сравнение вычислительной сложности обучения СНС

Набор данных	СНС	Веса	Соединения	% ошибок на тестовом множестве
Planetsnet	Planetsnet	264k	2324k	2.4
	CHC_1	150k	1670k	2.5
MNIST	LeNet-5	60k	340k	0.8
	CHC_2	42k	256k	0.7

8. Согласно правилу γ^5 выбирается элемент a_k, и заносится в Z_l,

9. Вычисляется число соединений:

$$Q_k^* = \sum W_{a_k} x_{i,j}^l \ , \ Q^* = Q^* + Q_k^* ,$$

число используемых весов:

$$M_k^* = W_{a_k} x_{i,j}^l , \ M^* = M^* + M_k^* .$$

10. Проверка условия $Q^* \le \frac{Q}{l}$, если выполняется, то $k = k + 1$, переход к шагу 6, если не выполняется, то $n = n + 1$, переход на шаг 5.

11. В подмножество Z_l заносится l полносвязных выходных нейронов, $Z = \{Z_1, \ldots, Z_l\}$.

12. Проверка модели на условие отсечения, если да, то $Z = \{Z_1, \ldots, Z_l\}$ заносится в $A^{-\text{СНС}}$, нет переход на шаг 13.

13. Полученная модель $Z = \{Z_1, \ldots, Z_l\}$ исключается из множества $A^{\text{СНС}}$, обучается на тестовом наборе данных, модель и результаты обучения P, P_1, P_2 сохраняются в базу данных под обозначением A^j.

14. Проверяется наличие неисследованных альтернатив $A^{\text{СНС}}$, если выполняется, переход на шаг 3, «нет» продолжение.

15. Выбирается конфигурация из базы данных A^j, для которой P — max.

4. Результаты экспериментов

Для проведения эксперимента выбраны получившие широкое распространение наборы обучающих данных MNIST и Planetsnet. Сравнения проводились на СНС LeNet-5 и СНС, представленной с набором данных Planetsnet. При создании CHC_1 и CHC_2 использовался предложенный алгоритм, в качестве элементов компоновки фильтры размерами 1×1, 3×3, 5×5, 7×7, 11×11, полносвязные слои, субдискредитация 2×2. Результаты экспериментов представлены в таблице 2.

Из табл. 2 видно, что представленный алгоритм позволяет автоматически подбирать состав архитектуры СНС. Большая разница по количеству весовых коэффициентов и соединений с сетью LeNet-5, объясняется прежде всего использованием приемов построения СНС, появившихся после создания LeNet-5. На наборе данных Planetsnet алгоритм показывает практически такую же точность, при меньшей вычислительной сложности.

Заключение

Предложенный алгоритм целесообразно использовать для автоматического подбора составных элементов СНС для решения различных задач, так как именно ручное проектирование конфигурации СНС занимает значительное время. Алгоритм предлагается использовать на Земле для подготовки СНС. Полученные нейронные сети затем переносятся в бортовую вычислительную систему, для автономного распознавания объектов на изображениях, получаемых оптическими датчиками. Наличие такой информации позволяет снизить зависимость бортовой системы управления БЛА от использования информационных каналов.

Одним из не очень существенных недостатков предложенного алгоритма является необходимость многократного обучения СНС при выборе конфигурации, оптимальной для используемого набора данных. Отметим, что использование распараллеливания обучения на современных видеокартах Nvidia позволяет значительно уменьшить время обучения нейронной сети. Кроме того, обучение СНС проводится на Земле и, как следствие, к длительности обучения СНС не предъявляются жесткие требования.

Дальнейшие исследования целесообразно продолжить в направлениях совершенствование правил компоновки элементов и отсечения неперспективных архитектур для уменьшения количества обучаемых сетей.

Литература

1. *Chitade A. Z.* Colour based image segmentation using k-means clustering // International Journal of Engineering Science and Technology. 2010. Vol. 2(10). Pp. 5319–5325.

2. Методы компьютерной обработки изображений / под ред. В. А. Сойфера. 2-е изд. М.: Физматлит, 2003. 784 с.

3. *Яковлев Е.Л., Хомоненко А.Д., Арчаков С.Н., Ерин А.А.* О выделении контуров объектов на изображениях при дистанционном зондировании Земли для обеспечения безопасности на транспорте // Сборник трудов Всероссийской научно-практической конференции

«Августин Бетанкур: от традиций к будущему инженерного образования». Санкт-Петербург, 2018. С. 6–10.

4. *Viola P., Jones M.J.* Robust Real-Time Face Detection // International Journal of Computer Vision. 2004. Vol. 57(2). Pp. 137–154.

5. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений: пер с англ. М.: Техносфера, 2005. 1072 с.

6. *Hu M.* Visual Pattern Recognition by Moment Invariants // IRE Trans. Inf. Theory. 1962. Vol. 8. Pp. 179–187.

7. *Старобинец Д.Ю., Хомоненко А.Д., Гаврилова Н.А.* Автоматический выбор параметров сжатия изображений с потерями на основе инвариантных моментов при дистанционном зондировании Земли // Современные проблемы дистанционного зондирования Земли из космоса. 2017. Т. 14. № 5. С. 26–36.

8. *Круглов В.В., Дли М.И., Голунов Р.Ю.* Нечеткая логика и искусственные нейронные сети. М.: Физматлит, 2001. 224 с.

9. *LeCun Y., Bottou L., Bengio Y., Haffner P.* Gradient-Based Learning Applied to Document Recognition // Proceedings of the IEEE. 1998. Vol. 86. No. 11. Pp. 2278–2324.

10. *LeCun Y*, Cortes C., *Burges C.J.C.* The MNIST database of handwritten digits. URL: http://yann.lecun.com/exdb/mnist/ (дата обращения 01.11.2018).

11. *Krizhevsky A., Sutskever I., Hinton G.E.* ImageNet Classification with Deep Convolutional Neural Networks // Proceedings of the 25th International Conference on Neural Information Processing Systems (NIPS'12). Advances in Neural Information Processing Systems 25 (Lake Tahoe, Nevada, 03–06 December 2012). 2012. Pp. 1097–1105.

12. *Szegedy C., Liu W., Jia Y., Sermanet P., Reed S.E., Anguelov D., Erhan D., Vanhoucke V., Rabinovich A.* Going Deeper with Convolutions / Cornel University Library. 2014. URL: http://arxiv.org/abs/ 1409.4842 (дата обращения 01.11.2018).

13. *He K., Zhang X., Ren S., Sun J.* Deep Residual Learning for Image Recognition. 2015. arXiv:1512.03385.

14. *Назаров А.В., Лоскутов А.И.* Нейросетевые алгоритмы прогнозирования и оптимизации систем. СПб.: Наука и Техника, 2003. 384 с.

15. *Смолицкий Х.Л., Ефимов В.В., Горбулин В.И. и др.* Методы синтеза структур нейронных сетей. СПб.: ВИККИ им. А. Можайского. 1993. 54 с.

16. *КоролевД.А., Суфиянов В.Г.* Нейроэволюционный подход к оптимизации внутренней структуры нейронных сетей // Вестник ТОГУ. 2007. № 4(7). С. 107–122.

17. *Тимофеева Н.К.* Один алгоритм компоновки БЭ корпуса ИМС // Алгоритмы и программы решения задач дискретной оптимизации. К.: ИК АН УССР, 1980. С. 2–14. URL: https://github.com/rhammell/planesnet-detector (дата обращения 01.11.2018).

THE RATIONALE FOR THE ARCHITECTURE OF THE CONVOLUTIONAL NEURAL NETWORK FOR OBJECT RECOGNITION ON IMAGES ON-BOARD COMPUTER SYSTEM

ANATOLIY D. KHOMONENKO
St-Petersburg, Russia, khomonenko@pgups.ru

EVGENY L. YAKOVLEV
St-Petersburg, Russia, evgen-1932@yandex.ru

KEYWORDS: convolutional neural network; autonomous recognition of objects on images; onboard computer system.

ABSTRACT

An approach is proposed to substantiate the architecture of a convolutional neural network (SNS), which provides improved performance in the number of weighting factors and connections while maintaining the accuracy of object recognition in images. Learning SNA with the selected architecture is implemented on Earth. After training, the neural network is used in onboard computing systems for autonomous recognition of objects in images. The analysis of the features of the construction of the SNA for the recognition of objects in images is carried out, and on its basis, limitations and rules for the development of new SNA are formulated. The formulation of the combinatorial optimization problem is formulated, a heuristic algorithm is proposed for solving this problem based on the rules of layout and cutting off unpromising SNA configurations. For the Planetsnet and MNIST test datasets, the results of computer experiments are presented and compared with existing SNA architectures by the number of weights, connections, and accuracy in% of errors on the test set. It is shown that the proposed algorithm allows you to choose a variant of the SNA architecture with a smaller number

of weighting factors and compounds with almost the same accuracy in% error solving the problem of recognizing objects in the image.

REFERENCES

1. Chitade A.Z. Colour based image segmentation using k-means clustering. *International Journal of Engineering Science and Technology*. 2010. Vol. 2(10). Pp. 5319–5325.

2. Soyfera V.A. (Ed.). *Metody komp'yuternoy obrabotki izobrazheniy* [Methods of computer image processing]. 2nd edition. Moscow: Fizmatlit, 2003. 784 p. (In Russian)

3. Yakovlev E.L., Khomonenko A.D., Archakov S.N., Erin A.A. O vydelenii konturov ob''ektov na izobrazheniyakh pri distantsionnom zondirovanii Zemli dlya obespecheniya bezopasnosti na transporte [About allocation of contours of objects on images at remote sensing of the Earth for safety on transport]. *Sbornik trudov Vserossiyskoy nauchno-prakticheskoy konferentsii "Avgustin Betankur: ot traditsiy k budushchemu inzhenernogo obrazovaniya"* [Proceedings of the all-Russian scientific-practical conference "Augustine Betancourt: from traditions to the future of engineering education"]. St. Petersburg, 2018. Pp. 6–10. (In Russian)

4. Viola P., Jones M.J. Robust Real-Time Face Detection. *International Journal of Computer Vision*. 2004. Vol. 57(2). Pp. 137–154.

5. Gonzalez R.C., Woods R.E. Digital Image Processing. 3rd edition. Prentice-Hall, 2007. 976 p.

6. Hu M. Visual Pattern Recognition by Moment Invariants. *IRE Trans. Inf. Theory*. 1962. Vol. 8. Pp. 179–187.

7. Starobinets D. Yu., Khomonenko A.D., Gavrilova N.A. Avtoma-ticheskiy vybor parametrov szhatiya izobrazheniy s poteryami na osnove invariantnykh momentov pri distantsionnom zondirovanii Zemli [Automatic selection of lost image compression options based on invariant moments in remote sensing of the Earth]. *Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa* [Modern problems of remote sensing of the Earth from space]. 2017. Vol. 14. No. 5. Pp. 26–36. (In Russian)

8. Kruglov V.V., Dli M.I., Golunov R. Yu. *Nechetkaya logika i iskusstvennye neyronnye seti* [Fuzzy logic and artificial neural networks]. Moscow: Fizmatlit, 2001. 224 p. (In Russian)

9. LeCun Y., Bottou L., Bengio Y., Haffner P. Gradient-Based Learning Applied to Document Recognition. *Proceedings of the IEEE*. 1998. Vol. 86. No. 11. Pp. 2278–2324.

10. LeCun Y, Cortes C., Burges C.J.C. The MNIST database of handwritten digits. URL: http://yann.lecun.com/exdb/mnist/ (date of accessed 01.11.2018).

11. Krizhevsky A., Sutskever I., Hinton G.E. ImageNet Classification with Deep Convolutional Neural Networks. *Proceedings of the 25th International Conference on Neural Information Processing Systems (NIPS'12). Advances in Neural Information Processing Systems 25 (Lake Tahoe, Nevada, 03–06 December 2012)*. 2012. Pp. 1097–1105.

12. Szegedy C., Liu W., Jia Y., Sermanet P., Reed S.E., Anguelov D., Erhan D., Vanhoucke V., Rabinovich A. Going Deeper with Convolutions / Cornel University Library. 2014. URL: http://arxiv.org/abs/ 1409.4842 (date of access 01.11.2018).

13. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition. 2015. arXiv:1512.03385.

14. Nazarov A.V., Loskutov A.I. Neyrosetevye algoritmy prognozirovaniya i optimizatsii sistem [Neural network algorithms of forecasting and optimization of systems]. St. Petersburg: Nauka i Tekhnika, 2003. 384 p. (In Russian)

15. Smolitskiy Kh.L., Efimov V.V., Gorbulin V.I. et al. *Metody sinteza struktur neyronnykh setey* [Methods for synthesis of structures of neural networks] St. Petersburg: VIKKI im. A. Mozhayskogo. 1993. 54 p. (In Russian)

16. Korolev D.A., Sufiyanov V.G. The neuroevolutionary ap-proach to optimization of inner structure of neural nets. *Bulletin of TOGU*. 2007. No. 4(7). Pp. 107–122. (In Russian)

17. Timofeeva N.K. Odin algoritm komponovki BE k korpusa IMS [One algorithm of be layout to the case of IC]. [Algorithms and programs for solving discrete optimization problems]. Kiev: IK AN USSR, 1980. Pp. 2–14. URL: https://github.com/rhammell/planesnet-detector (date of accessed 01.11.2018). (In Russian)

INFORMATION ABOUT AUTHORS:

Khomonenko A.D., PhD, Professor, Head of the Department of Information and Computing systems of Emperor Alexander I St. Petersburg state transport university, professor at the Department of mathematical and software of Military Space Academy;

Yakovlev E.L., Adjunct at the Department of mathematical and software of Military Space Academy.

For citation: Khomonenko A.D., Yakovlev E.L. The rationale for the architecture of the convolutional neural network for object recognition on images on-board computer system. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 86–93. doi: 10.24411/2409-5419-2018-10190 (In Russian)

doi: 10.24411/2409-5419-2018-10191

THE OPTIMIZING METHOD OF REPAIRING ALLOCATION FOR ARMING SAMPLES AND MILITARY EQUIPMENT TO CARRY OUT RESOURCESREGENERATIVE REPAIRING ACCORDING TO THE TECHNICAL CONDITION

ROMAN V. DOPIRA[1]

DMITRY YU. BREZHNEV[2]

DMITRY V. YAGOLNIKOV[3]

VADIM B. SHAROGLAZOV[4]

ABSTRACT

The lag in new arming samples and military equipment production due to lag of their wear makes the resourcesregenerative repairing according to technical condition more necessary that provide technical preparedness level maintenance and required equipment margin. The key aspect of resourcesregenerative repairing according to technical condition realization is the need for military equipment repairing and repairing authorities' possibilities reconciliation procedure. The planning of repairing becomes more difficult for the planning of arming and military equipment replacement, so this task requires mathematical solution methods. The peculiarity in solving this task is the fact that there are objects with different repair size and repairing possibilities among all the objects of this kind both in stationary and army conditions and repairing authorities are mobile and stationary subdivisions with different productive capabilities. The task is to find out how to distribute military equipment samples between repairing authorities so that the costs would be minimal at a certain planning point. In formalized shape this is a combinatorial optimization task in mathematical optimization area which is characterized as generalized assignment problem with additional conditions and is NP-complete. The algorithm of distribution is based on solution of the Boolean linear programming task using the Hungarian method with repair facility's queuing recalculation. The task decomposition in several private subtasks that are accomplished in a chain is suggested to reduce the tusk dimension. Such a method allows us to get an optimal plan of resourcesregenerative repairing according to technical condition realization with minimal costs and on time. The programming task realization and the suggested algorithm will allow getting an instrument of Event Management in resource replacement to a variable degree that will provide repairing authorities management.

Information about authors:

[1]PhD, Full Professor, Senior Research Officer of the Military academy of aerospace defense of Military Space Academy, Tver, Russia, rvdopira@yandex.ru

[2]PhD, Doctoral Candidate of the Military academy of aerospace defense, Tver, Russia, dimanbreg@mail.ru

[3]PhD, Lecture at the Department of tactics and arming radio engineering forces of the Military academy of aerospace defense, Tver, Russia, yagolnikov_dv@mail.ru

[4]lecturer at the Department of the organization of operation and technical providing arms of military and special equipment of the Military Space Academy, St Petersburg, Russia, sh.vadim.b@yandex.ru

KEYWORDS: arming and military equipment of air defense; repairing according to technical condition; equipment management; Boolean linear programming, Hungarian method.

For citation: Dopira R.V., Brezhnev D.Yu., Yagolnikov D.V., Sharoglazov V.B. The optimizing method of repairing allocation for arming samples and military equipment to carry out resourcesregenerative repairing according to the technical condition. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 94–99. doi: 10.24411/2409-5419-2018-10191

Army equipping with modern military equipment samples requires considerable financial allocations. The country's budget capacity makes us search for solutions that allow arming and military equipment maintenance, technical condition and military equipment life margin. At the same time it is rather difficult nowadays to reach the desired level of new military equipment in short time period considering industrial capacity and country's budget allocation limits. Especially concerning high-tech arming samples which include air defense system and radar stations that are operational with air defense troops. That's why we need a complex approach in the condition of defense allocations that allows finding a sensible compromise between industrial capacity for new military samples delivery and troops and service organizations' capacity to maintain available equipment according to resource margin included.

The military equipment management is one of the most important management operation system functions and includes several tasks, the main of them are:

1) planning, order and organization of military equipment delivery as part of State arming program and State defense order;

2) planning, organization and control of the resource rate put into action in military equipment in all kinds of storage included;

3) planning, organization and control of resources regenerative repairing realization;

4) organization of working military equipment life extension with operating time close or equal to the appointed resource before resources regenerative repairing realization (retirement).

In this article, we consider one of the solutions to the third task — planning, organization and control of resources regenerative repairing realization.

To solve this task in military equipment repairing system that is a subsystem of technical service and repairing system a regenerative system of air defense military resource was organized and works now.

A regenerative system of air defense military resource is multilevel and is a body of interrelated performers, facilities and documentation used for resources regenerative repairing realization.

The structure of the regenerative system of air defense military resource allows operation management authorities to plan and to organize different variants of resources regeneration differing in resources regenerative level, repairing location, enlisted performers, facilities and documentation:

1. Variants with complete and close to complete arming and military equipment resources regeneration performing capital resources regenerative repairing (with or without modernization) in stationary institutions in-house using their funds, operational documentation, construction repair documentation for capital repair realization, engineering construction documentation while carrying out modernization and defense industry bulletins. Stationary institutions are industrial establishments (institutions-developers and institutions- manufacturers of arming and military equipment) and defense-industrial sector repairing institutions for short.

2. Variants with partial military equipment resources regeneration performing repairing according to technical condition:

– in stationary institutions in-house using funds of operational documentation institutions, repair documentation and defense industry bulletins;

– in military equipment operation places using force-account mobile repairing teams ability of stationary institutions, circulating and reserve funds of institutions or force-account operational staff and repairing institutions ability with or without mobile repairing teams ability of stationary institutions using military equipment, means of stationary and mobile workshop repair in military units, operational documentation, repair documentation and defense industry bulletins.

All the resources regenerative repairs are planned and can be performed both according to age repair and technical condition.

Note that the lag in new arming samples and military equipment production due to lag of their wear makes the resources regenerative repairing according to technical condition more necessary, especially applied to the military equipment samples that have already been routinely capitally repaired. The idea of resources regenerative repairing according to technical condition is to perform repairing service that are directed to technical samples work capability repair and partial resource replacement according to factual technical condition of resource elements [1]. We understand a resource element here as an element of military equipment sample the nonremovable defect of which generally determines the sample limiting state and its lifetime generally determines military equipment sample lifetime. The military equipment sample has several resource elements, as a rule, every of them limits its lifetime on the whole.

One of the resources regenerative repairing realization key problems is the matching procedure of need for repairing military samples after technical diagnosis and repairing authorities' capability. At the same time repair planning becomes more difficult for necessity to perform both army repairs (in military equipment operation places using force-account mobile repairing teams' ability of stationary institutions from repairing authorities) and depot repair connected with military equipment relocation to the places of repair realization in stationary conditions. High dimension of event planning task involves mathematical methods of decision-making for resources regenerative repairing according to technical condition organization [2].

Now we will formulate the task solution specification of the military equipment optimal distribution between repair authorities while repair planning.

Let the range of repair authorities be R, each of which includes several mobile repairing teams B and one stationary repair section for military equipment samples repairing in depot conditions.

Let according to results of technical diagnosis determine the list of the samples N which have resource elements in a damage wear condition. At the same time we know the damaged resource elements nomenclature of every n-sample ψ_n and the elements number of every nomenclature $l_{\text{Ё}}^n$. Note that the range of resource elements nomenclatures Ψ includes subset of such resource elements F, repair of which is possible only in depot conditions $F \subseteq \Psi$. Other elements of set Ψ make the subset $E = \Psi \backslash F$ and can be repaired both in depot and army conditions.

Thus the set of military equipment samples N that needs repairing is represented by subsets N_1 (the samples are repaired only in depot conditions) и N_2 (the samples are repaired both in depot and army conditions): $N_1 \subseteq N$, $N_2 \subseteq N$, $N_2 = N \backslash N_1$.

The task is to search for such a variant of military samples distribution between repairing authorities and mobile repairing teams whereby we have minimal costs connected with repair realization at this planning stage.

In a formalized shape we can perform the task of optimal military samples distribution this way: there is a set of repair samples N so that $N = N_1 \cap N_2$. At the same time $N_1 = \{n_m\}$, $N_2 = \{n_k\}$, where nm — complex of set N_1 elements, n_k — complex of set N_2 elements; there is the set of repairing channels $Q = \{q_1, q_2, \ldots q_j, \ldots q_s\}$, at the same time the capacity of the set $|Q|$ can be determined by

$$|Q| = s = \sum_{r=1}^{R} B_r + R, \qquad (1)$$

where B_r — the quantity of mobile repairing teams in r-th repairing authorities.

We need to distribute samples set N between repair channels Q so that the whole cost of repairing C be minimal

$$C(X) = \sum_{n=1}^{N} \sum_{q=1}^{|Q|} \left[x_{nq} c_{nq} \right] \xrightarrow[X]{} \min, \qquad (2)$$

to certain constraints

$$\sum_{n=1}^{N} \sum_{q=1}^{|Q|} \left[x_{nq} \tau_{nq} \right] \le {}'' {}_p, \qquad (3)$$

$$\sum_{n=1}^{N} x_{nq} = 1, \quad \forall q = \overline{1,s}, \qquad (4)$$

where $X = \left\| x_{nq} \right\|_{n=\overline{1,N};\ q=\overline{1,s}}$ — a sought-for matrix of functions for military equipment repair realization by repairing authorities the elements of which are determined in the form of Boolean variables:

$$x_{nq} = \begin{cases} 1, & \text{nominating } n-\text{th sample } q\text{-th repair canal} \\ 0, & \text{otherwise} \end{cases}, \qquad (5)$$

c_{nq} — repair cost of n-th military sample in q-th repair channel considering logistic operations connected with relocation of samples or mobile repairing teams; τ_{nq} — time spending for repair realization of n-th military sample in q-th repair channel considering logistic operations connected with relocation of samples or mobile repairing teams; T_p — duration of planning period.

The limit (3) provides with repair carrying-out within the directive time and means that one repairing channel can be designated to repair a number of military equipment samples during a certain planning period $T_p = [0, T]$ considering relocation time (of samples or mobile repairing teams) and repairing time. The limit (4) means that the repairing of each n-th military sample can be performed only by one q-th repair channel.

Thus, the formulated task is formalized and is in mathematical form: the desired function and its corresponding limits are discovered.

In a formalized shape the task is the problem of combinatorial optimization in mathematical optimization area. We can also characterize it as a generalized assignment problem with additional limits. It is NP-complete [3] and to solve such tasks specific algorithms based on combinatorics, graphs, etc are worked out [4,5].

We can solve formulated task using exact methods, such as branch and bound method [6–9] or Hungarian method [10–12].

In case of using branch and bound method before the start of branching and tree traversal assessment we recommend to perform branching levels presorting considering limit (3) [13]. Branching levels presorting is especially necessary for high task dimension as it helps to reduce level exhaustion. Nevertheless, one of the branch and bound method disadvantages is high computational complexity and computational burden [14] as one should keep in mind the results of prior level tops assessment while traversing the tree.

The algorithm of Hungarian method allows solving the task in polynomial time [15].

We can convert the task (1–5) into Boolean linear programming task using the Hungarian method for its solution.

In this case the main difficulty in working out the algorithm of its solution is connected with the presence of repairing specification subsets in the range of samples N and the range of repair channels Q which limit the usage of linear programming algorithms and also limits (3) and (5) where repairing queue size is specified in each repairing channel in planning time.

Thereby the task decomposition in several private subtasks that are accomplished in a chain is suggested to reduce the tusk dimension.

At the first stage, we consider elements of N_1 set the repairing necessity of which is defined by resource elements

damage wear of nomenclature F. At this stage, we solve the task of sample distribution between repairing authorities in the following sequence:

Step 1. Input data about allocated samples and repairing channels of stationary type (of sets N_1 and R).

Step 2. Formation of matrix input data $\left\|c_{nq}\right\|_{n=\overline{1,N_1};q=\overline{1,R}}$ and $\left\|\tau_{nq}\right\|_{n=\overline{1,N_1};q=\overline{1,R}}$ sized $N_1 \times R$ that match cost and duration of repairing between samples and stationary-typed repair channels.

Step 3. The set-up of initial position allocation cycle-counter (iterations) (n = 1) and preparing data for the first military samples distribution between stationary-typed repair channels.

Step 4. Solving of the Boolean linear programming task (2)–(6) using Hungarian method [6].

Step 5.Testing conditions in which the quantity of distributed military samples corresponds the quantity of repair channels:

if $N_1 = K$, then we found the solution, go to step 12;

if $N_1 < K$, then the solution isn't found, find the quantity of free channels ($R_{fr}(n+1) = R\text{-}R_{\text{dis}}(n)$) for their further distribution at the second stage and go to step 12;

if $N_1 > K$, then military samples queue is formed, test condition (3) and if it works go to the next step. If it doesn't work the rest of the samples are to be repaired at the next planning stage.

Step 6. Choose one allocation for every repair channel for derived solution.

Step 7. Exclude the derived set of military samples allocations from the input set and form a new set of samples for further distribution iteration ($N_1(n+1) = N_1 \backslash N_1(n)$).

Step 8. Correction of matrix sizes $\left\|c_{nq}\right\|$ and $\left\|\tau_{nq}\right\|$ for further distribution iteration. Thereby exclude lines from matrix according to step 7 and columns if condition 3 doesn't work for corresponding repair channels.

Step 9. Recalculate repair time of each sample for each repair channel in matrix $\left\|\tau_{nq}\right\|$ adding military samples repair time distributed to these repair channels during current iteration.

Step 10. Go to further iteration ($n = n + 1$).

Step 11. Go to step 4.

Step 12. Stop calculating. Form the final variant of samples distribution plan between stationary repair channels.

At the second stage we consider elements of N_2 set the repairing necessity of which is defined by resource elements damage wear of nomenclature E and elements of Q set, the list of which is formed according to results of the first stage.

Military samples distribution sequence is analogic to the first stage sequence with refinements in some steps.

At the first step the quantity of set Q elements is defined according to

$$S = \sum_{r=1}^{R} B_r + R_{fr}. \qquad (6)$$

In this case we form the list of repair channels which include not only mobile repairing teams but also stationary repair authorities from samples that aren't used for repairing of N_2 set.

At the second step we form matrix input data $\left\|c_{nq}\right\|_{n=\overline{1,N_2};q=\overline{1,S}}$ and $\left\|\tau_{nq}\right\|_{n=\overline{1,N_2};q=\overline{1,S}}$ sized $N_2 \times S$. Note that while forming this matrix in cells corresponding to samples repairing in stationary repair channels we should indicate cost of this repairing and repair time considering military equipment delivery duration to the repair location. Knowing in advance that repair cost in stationary conditions is much more expensive and a longer time than army repair, the algorithm will automatically give assignments to stationary repair channels in case of mobile repairing teams deficit at the bottom of priority.

The rest of the steps are accomplished analogically.

At the third stage we unite derived assignments and form a free repair plan.

Thus the introduced method of task solution allows us to get an optimal plan of resources regenerative repairing according to technical condition realization with minimal costs and on time.

The programming task realization and the suggested algorithm will allow getting an instrument of Event Management in resource replacement to a variable degree (depending on factual condition of resource elements) that will provide mobile repairing teams and stationary industrial repair authorities management.

The suggested method considerably reduce the time of repair planning problem solution and can be used in automatical system of technical troops maintenance management.

References

1. Pronikov A. S. *Parametricheskaya nadezhost' mashin* [Parametric reliability of machines]. Moscow: Moscow State Technical University named after Bauman Publ., 2002. 560 p. (In Russian)

2. Dopira R. V., Smolyakov A. A., Popov A. I., Scherbinko A. V. Planirovanie upravleniya resursom radioelektronnoy tehniki PVO VVS [Planning the management of the air force electronic air defense resource]. *Remont, Vosstanovlenie, Modernizatsiya* [Repair, Reconditioning, Modernization]. 2006. No. 5. Pp. 2–5. (In Russian)

3. Kellerer H., Pferschy U., Pisinger D. *Knapsack Problems*. Springer Verlag, 2005. p. ISBN3–540–40286–1.

4. Garey M. R., Johnson D. S. *Computers and Intractability. A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979. 347 p.

5. Lazarev A. A. *Teoriya raspisaniy. Otsenki absoluytnoy pogreshnosti i shema priblizhennogo resheniya zadach teorii raspisaniy* [Schedule theory. Estimates of the absolute error and the scheme of the approximate solution of the problems of the theory of schedules]. Moscow: MIPT Publ., 2008. 222 p. (In Russian)

6. Land A.H., Doig A. G. An automatic method of solving discrete programming problems. *Econometrica*. 1960. Vol. 28. Pp. 497–520.

7. Kovalev M. M. *Diskretnaya optimizatsiya (tselochislennoe programmirovanie)* [Discrete optimization (integer programming)]. Ed. 2nd. Moscow: Editorial URSS, 2003. 192 p. ISBN5–354–00499–3 (In Russian)

8. Sergienko I. V. (Ed.). *Matematicheskie modeli I metody resheniya zadach diskretnoy optimizatsii* [Mathematical models and methods for solving discrete optimization problems]. 2nd ed. Kiev: Sciences. Dumka, 1988. 472 p. (In Russian)

9. Bunday B. D. *Basic Linear Programming*. London, Edward Arnold, 1984. 172 p.

10. Kuhn H. W. The Hungarian Method for the assignment problem. *Naval Research Logistics Quarterly*. 1955. No. 2. Pp. 83–97.

11. Yudin D. B., Golshtein E. G. *Zadachi I metody lineynogo programmirovaniya* [Tasks and methods of linear programming]. Moscow: Soviet Radio, 1961. 494 p. (In Russian)

12. Zholobov D. A. *Vvedenie v matematicheskoe programmirovanie* [Introduction to math programming]. Moscow: MEPhI Publ., 2008. 376 p. (In Russian)

13. Tsvirkun A. D. *Osnovy sinteza struktury slozhnyh sistem* [Basics of the synthesis of the structure of complex systems]. Moscow: Science, 1982. 200 p. (In Russian)

14. Novikov F. A. *Diskretnaya matematika dlya programmistov* [Discrete mathematics for programmers]. Saint Petersburg: Peter, 2003. 304 p. (In Russian)

15. Munkres J. Algorithms for the Assignment and Transportation Problems. *Journal of the Society for Industrial and Applied Mathematics*. 1957. No. 5(1). Pp. 32–38.

МЕТОД ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ ОБРАЗЦОВ ВООРУЖЕНИЯ И ВОЕННОЙ ТЕХНИКИ ПО РЕМОНТНЫМ ОРГАНАМ ДЛЯ ПРОВЕДЕНИЯ РЕСУРСОВОССТАНАВЛИВАЮЩИХ РЕМОНТОВ ПО ТЕХНИЧЕСКОМУ СОСТОЯНИЮ

ДОПИРА Роман Викторович,
г. Тверь, Россия, rvdopira@yandex.ru

БРЕЖНЕВ Дмитрий Юрьевич,
г. Тверь, Россия, dimanbreg@mail.ru

ЯГОЛЬНИКОВ Дмитрий Владимирович,
г. Тверь, Россия, yagolnikov_dv@mail.ru

ШАРОГЛАЗОВ Вадим Борисович,
г. Санкт-Петербург, Россия, sh.vadim.b@yandex.ru

КЛЮЧЕВЫЕ СЛОВА: вооружения и военной техники противовоздушной обороны; ремонт по техническому состоянию; управление ресурсом техники; линейное булево программирование; венгерский метод.

АННОТАЦИЯ

Отставание темпов производства новых образцов вооружения и военной техники от темпов их старения обусловливают необходимость более широкого применения ресурсовосстанавливающих ремонтов по техническому состоянию, обеспечивающих поддержание уровня технической готовности и требуемый запас ресурса техники. Ключевым вопросом проведения ресурсовосстанавливающих ремонтов по техническому состоянию является процедура согласования потребностей в ремонте образцов вооружения и военной техники с возможностями ремонтных органов. Планирование ремонта осложняется большой размерностью задачи планирования мероприятий по восполнению ресурса вооружения и военной техники и требует применения математических методов её решения. Особенностью решения задачи является наличие в составе множества распределяемых объектов ремонта образцов с различным объемом ремонта и возможностью его проведения, как в стационарных, так и в войсковых условиях, а ремонтные органы представлены подразделениями

в мобильном и стационарном вариантах с различными производственными возможностями. Задача заключается в поиске варианта распределения образцов вооружения и военной техники между ремонтными органами, при котором обеспечиваются минимальные экономические затраты, связанные с проведением их ремонта на заданном интервале планирования. В формализованном виде задача представляет собой задачу комбинаторной оптимизации в области математической оптимизации, характеризуется как обобщенная задача о назначениях с дополнительными условиями и является NP-полной задачей. В основу алгоритма распределения образцов вооружения между ремонтными органами положено решение задачи линейного булевого программирования с применением венгерского метода, дополненного процедурой пересчета длины очереди на ремонтных предприятиях. Для снижения размерности решаемой задачи предложено провести ее декомпозицию на ряд частных подзадач, выполняемых в определенной последовательности. Представленный метод решения задачи распределения образцов вооружения и военной техники позволяет получить оптимальный план проведения ресурсовосстанавливающих ремонтов по техническому состоянию при минимуме затрат на их проведения в требуемые сроки. Программная реализация данной задачи с использованием предложенного алгоритма позволит получить инструмент управления мероприятиями по восполнению ресурса различной степени, обеспечивающий рациональное использование ремонтных органов.

СВЕДЕНИЯ ОБ АВТОРАХ:

Допира Р.В., д.т.н., профессор, старший научный сотрудник Военной академии воздушно-космической обороны имени Маршала Советского Союза Г.К. Жукова;

Брежнев Д.Ю., к.т.н., докторант Военной академии воздушно-космической обороны имени маршала Советского Союза Г.К. Жукова;

Ягольников Д.В., к.т.н., преподаватель кафедры тактики и вооружения РТВ Военной академии воздушно-космической обороны имени маршала Советского Союза Г.К. Жукова;

Шароглазов В.Б., преподаватель кафедры организации эксплуатации и технического обеспечения ВВСТ Военно-космической академии имени А. Ф. Можайского.

Для цитирования: *Допира Р.В., Брежнев Д.Ю., Ягольников Д.В., Шароглазов В.Б.* Метод оптимизации распределения образцов вооружения и военной техники по ремонтным органам для проведения ресурсовосстанавливающих ремонтов по техническому состоянию // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 94–99. doi: 10.24411/2409-5419-2018-10191 (Англ.)

doi: 10.24411/2409-5419-2018-10192

MODELS AND METHODS OF RESOURCE ALLOCATION OF INFOCOMMUNICATION SYSTEM IN CLOUD DATA CENTERS

ANDREW V. TOUTOV

Information about author:

Senior Lecturer of the Moscow technical university of communications and informatics, Moscow, Russia, andrew_vidnoe@mail.ru

ABSTRACT

The main problem of modern data centers is the colossal power consumption. In order to minimize power consumption it is necessary to improve methods for resources allocation, while ensuring a high quality of service. Reallocation of resources in the cloud data center occurs through live migration of virtual machines, which additionally loads the system and interrupts monitoring of servers. Currently, there is a large number of works devoted to individual issues of optimal allocation and resource management of cloud data centers. However, in known works there is no complete cycle of work. This paper proposes models and methods for a complete cycle of optimization and resource management of the cloud data center infocommunication system. In particular, the model for the initial placement of virtual machines in the form of a multicriteria optimization problem and the method for solving it are proposed. A two-level resource management system is presented, which includes local and global controllers. The local controller monitors the load and temperature of servers and makes a prediction for the next monitoring window. For prediction, it is suggested to use the method of group method of data handling (GMDH). To determine the size of the monitoring window two types of live migration have been studied and the method for calculating total migration time has been proposed, based on finding an analytical expression for the probability density. For SaaS and PaaS services which use horizontal scaling, a model of two-criteria optimization of the number of virtual machines in clusters of a large multi-tier application is proposed. It is suggested to solve this by a combined method of successive concessions and restrictions.

KEYWORDS: resource management; cloud computing; virtual machine placement; live migration; data center; resource allocation.

For citation: Tutov A.V. Models and methods of resources allocation of infocommunication system in cloud data centers. *H&ES Research*. 2018. Vol. 10. No. 6. Pp. 100–00. doi: 10.24411/2409-5419-2018-10192

Introduction

In recent years, the activities of telecom operators have undergone a digital transformation, in which telecommunications operators have to provide digital services in data centers. Cloud computing is one of the most important areas. It is based on virtualization technology that allows to implement the basic requirements of cloud services, such as the use of resources on demand and resource elasticity, through the horizontal and vertical scaling of applications and live migration of virtual machines (VM).

The infrastructure and architectural solutions of data centers focused on cloud services are not fundamentally different from traditional virtualized data centers. However, evolution to cloud data centers at the same time puts more stringent requirements for the performance of the infocommunication system, cooling systems and power supplies in a high-density environment.

The main problem of modern data centers is the consumption of colossal amounts of power, a significant part of which goes to auxiliary systems, in particular a cooling system, which begins to work hard in the event of uneven temperature distribution in the hall. In addition, despite the fact that many data centers are already filled, a significant part of the computing resources is used inefficiently.

To minimize power consumption, heat generation, uniform resource utilization and provide service quality according to SLA agreements, it is necessary to improve the resource allocation process, including methods for initial and dynamic VM placement, as well as scaling.

Reallocation of resources in the cloud data center occurs by VM migration, which is a costly operation, additionally loading network and servers, affecting the quality of services and server monitoring. Therefore, in order to perform effective monitoring and forecasting the state of servers, it is necessary to estimate the total migration time of VMs.

Currently, there is a large number of works devoted to individual issues of optimal allocation and management of resources of cloud data centers. The problems of the initial placement are considered in papers [1–6], dynamic resource allocation in [7–11], scaling issues in [12, 13], live migration of virtual machines in [14–16]. However, in known works there is no complete cycle of work on optimization and management of cloud data center resources.

In this paper, proposed models and methods the proposed models and methods constitute a full cycle optimization and resource management of the cloud data center infocommunication system, including initial and dynamic virtual machine placement, method for forecasting server overloads and underloads, and method for calculating the duration of VM live migration to select the size of the monitoring window.

Initial placement

Depending on the initial state of the data center, the VM allocation methods are divided into two types: initial and dynamic placement.

The initial placement occurs when a group of virtual machines are located in the data center for the first time or transferred from one data center to another. In most works devoted to optimization of the initial placement, the following statement is used: there are M different physical servers connected to the network, each of which is characterized by the performance of the processor (CPU) and the amount of memory (RAM). Also, the network bandwidth and the load coming to each server are known. In addition, N virtual machines are specified, the characteristics of which are ordered by users. It is required to consolidate virtual machines on physical servers, so that energy consumption, unused resources, uneven heat dissipation and violation of SLA-agreements are minimized. To solve this problem, heuristic algorithms FFD and BFD are proposed, as well as their modifications [1]. Evolution algorithms are also used to obtain results on this problem [3–5].

Multicriteria problem is solved by constructing the generalized criterion [5]. In [6] it was shown that the best result can be achieved using a combined method of successive concessions and restrictions [17].

Horizontal scaling

One of the most important advantages of cloud computing is resource elasticity, i.e. the ability to add resources to the application and pay only for consumed resources. To scale resources in cloud computing, virtual machines that run the same application are clustered. Horizontal scaling is the process of adding or removing VMs from a cluster. Cloud providers of SaaS and PaaS services negotiate into service level agreements (SLA) with users, in which one of the indicators is the average response time for a query or the maximum response time for a given percentage of requests. Currently, the predominant architecture of Web applications is a multi-tier architecture, implying the use of Web servers for data representation, application servers for implementing application logic and database servers for managing databases. Schematically, a cloud with multi-tiered applications is shown in fig. 1.

Such a cloud is modeled as an open queuing network, where each node is a cluster of virtual machines such as m/G/1/PS. The discipline of service is the processor sharing (PS). For such a network, the expression to determine mean response time was obtained in [12]. Since the number of directly running virtual machines in the cluster can vary depending on the load, it is possible to determine the optimal number of virtual machines in clusters of a multi-tier application by the criteria of minimum costs and maximum capacity:

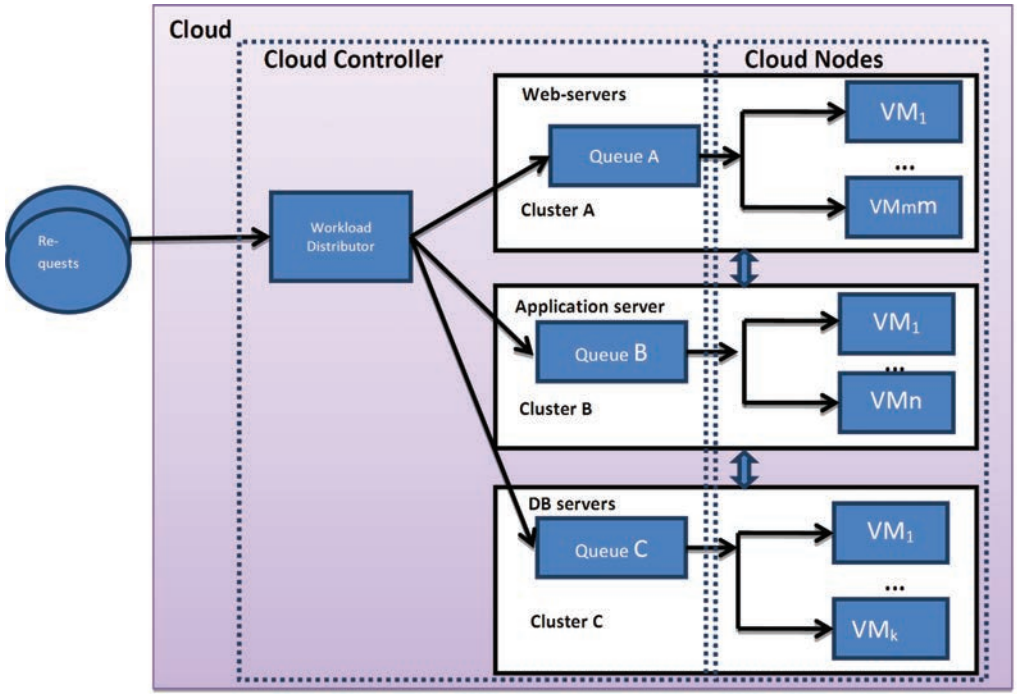


Fig. 1. Cloud data center with multi-tier applications.

$$\min_{\{S_1,...,S_C\}} F_{TCO}(S_1,...,S_C) = \sum_{c=1}^{C} TCO_c \cdot S_c;$$

$$\max_{\{S_1,...,S_C\}} F_{TP}(S_1,...,S_C) = \sum_{c=1}^{C} \frac{S_c}{\frac{1}{K}\sum_{k=1}^{K} m_c^k},$$

under constraints

$$\sum_{c=1}^{C} \frac{\lambda_c^k}{\lambda^k} \frac{m_c^k}{S_c - q_c} \le T_{SLA}^k,$$

$$k = 1,. . ., K, \quad q_c < S_c \le S_c^{\max}, \quad c = 1, \ldots, C.$$

where C — the number of virtual clusters of data centers;

K —the number of query classes;

S_c — number of servers in the cluster c;

F_{TP} — criterion of the data center throughput;

F_{TCO} — criterion of total cost of ownership of data center servers;

TCO_c — total cost of ownership of one cluster server c;

q_c — nominal cluster load with one server at load λ_c;

m_c^k — the average processing time of a class k query by a weakly loaded cluster server c;

$\frac{\lambda_c^k}{\lambda^k}$ — the average number of visits to the cluster c with the query of class k during its time in the system;

λ_c^k — the arrival rate of query of class k in the cluster c;

λ^k — the arrival rate of query of class k in the system;

T_{SLA}^k — restriction on the average response time for a query of class k specified in the SLA-agreement;

$S_c^{\max}$ — the maximum possible number of servers in the cluster c.

This problem is proposed to be solved by a combined method of successive concessions and restrictions [17].

Dynamic allocation

Data centers must provide sufficient resources for the hosted applications. The operating conditions can be characterized by significant load changes. In cases where these changes affect application performance, the resource management system has to dynamically reallocate resources by redistributing virtual machines between physical servers without loss of VM availability. For cloud providers, the most important criteria are server power consumption, cooling costs, and uniform resource utilization.

Dynamic resource allocation is implemented by the resource management system and is based on the use of virtual machine migration depending on the current operating conditions of the system. The resource management system should answer the following questions:

- When to migrate VMs?
- Which VMs to choose for migration?
- Where to migrate the VMs?

The cloud resource management system has a two-tier architecture consisting of global and local controllers (fig. 2) [7].

Local controllers analyze the state of the physical servers on which they are located and determine the possible underload, overload and overheat states based on the forecast for the next observation window, which is performed using the group method of data handling (GMDH). If one of the following conditions is detected, the local controller reports this to the global controller, which selects the destination server to which the VM will be migrated.

In this system, local controllers decide which VM and when it should be moved. While global controller answers the question where to move the VM. To do this, the local controllers constantly analyze the monitoring system data, and in case of output of the working model parameters beyond the permissible level, they inform the global controller that activates the migration process of virtual machines.

Verification of the system indicators is carried out sequentially, in accordance with the importance of the criteria (overheating, overload, underload of the host). The monitoring process is carried out continuously, even during the migration of the virtual machine. Priority criteria can be changed by the system administrator, but due to their inconsistency, the verification phase should remain sequential (fig. 3).

In case of condition for VM migration, the global controller determines the VM on the problem hosts and starts the algorithm for finding the optimal destination host. The destination host selection is also a sequential step, where each application is processed in the queue order. After determining the destination host and starting the migration process, this physical server is temporarily removed from the list of available nodes until the end of migration.

The process of dynamic placement of virtual machines includes monitoring and forecasting the state of servers. As a method of forecasting, it is suggested to use the group method of data handling (GMDH) [7, 18].

It was noted that the criterion for choosing the optimal structure of the model strongly affects the quality of forecasting. The best results were obtained with the choice of the model by minimizing the criterion of regularity at the last two points of the examination sample. This allows us to take into account the latest sample data for a more accurate short-term forecast. To test the effectiveness of the dynamic allocation of resources with the proposed forecasting method, a simulation model was developed using the CloudSim package [19]. It is shown that the GMDH combinatorial algorithm for predicting the characteristics of destination hosts for all samples yields

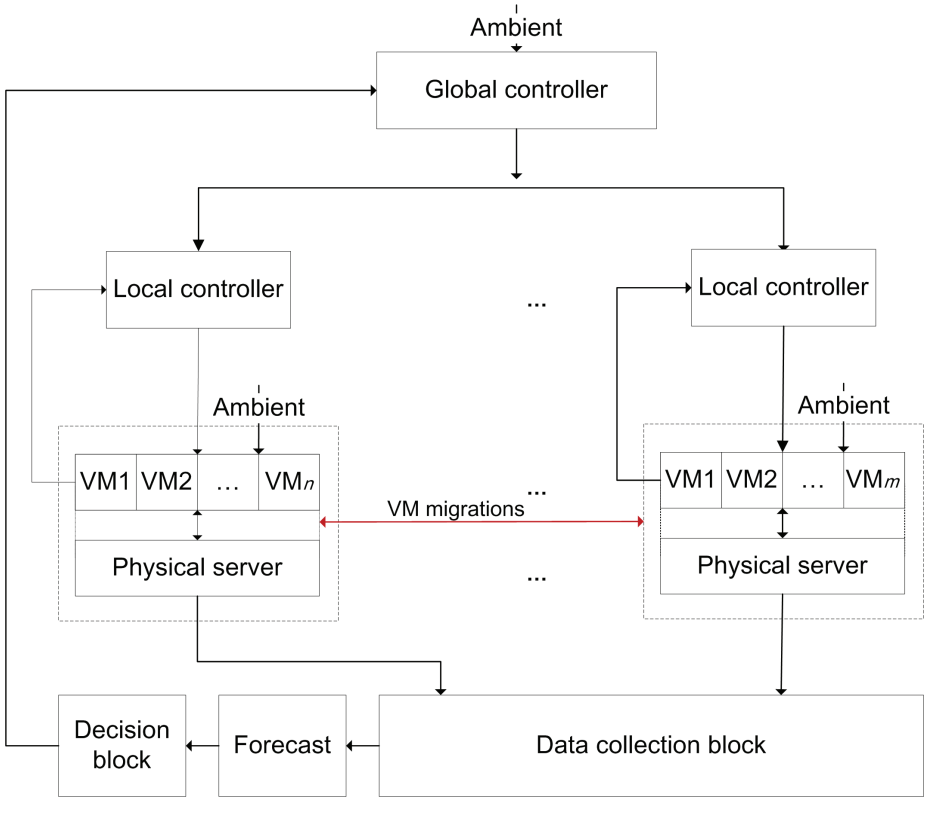


Fig. 2. Two-tier system for managing the resources of the cloud data center

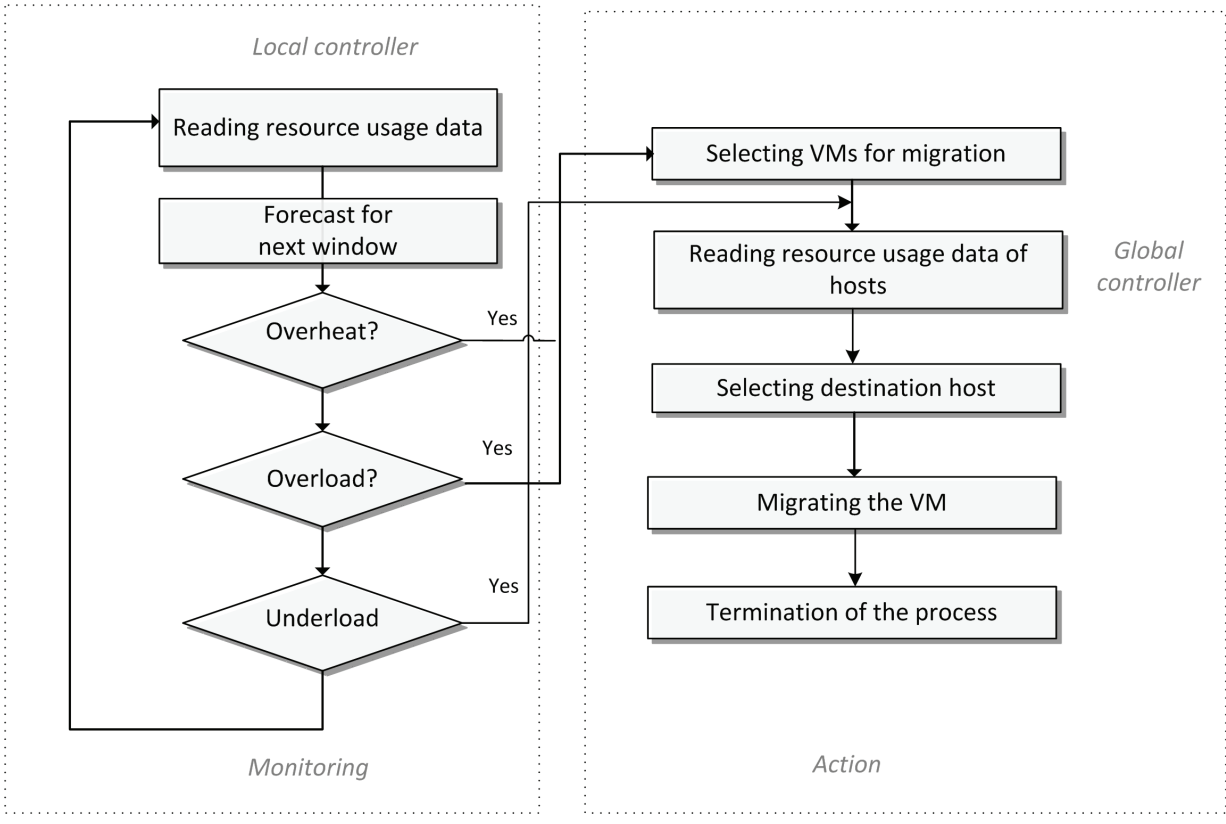


Fig. 3. The algorithm of controller operation

results not worse than those published earlier, obtained by the local regression method [8].

The quality of forecast depends on the correctness of the data collected by the monitoring subsystem. Since migration further burdens the network and servers on both sides, it is necessary to estimate the migration time, which has a wide spread depending on the application [20]. In [21] it was shown that in order for migration not to affect the monitoring process for servers, the size of the monitoring window should be larger than the total migration time of the migration. A method is proposed for calculating the total migration time of migration on the basis of finding the analytical expression for the probability density of total migration time.

Method for calculation the total migration time

The calculation method is justified in [22] and consists of a number of stages.

1. Collect data on the number of migrations N and the number of elementary operations in the migration X for the periods of observations T. The elementary operation of the migration process is the minimum deterministic part of it, denoted $t_{\min}$

$$t_{\min} = T_P + T_R + T_{SC} + T_C + T_A,$$

where T_P — the initialization time;

T_R — time for resource reservation;

T_{SC} — time for stop and copy phase;

T_C — time for commitment;

T_A — time for activation.

2. Estimate the parameters of the distributions of the number of migrations and the number of elementary operations

λ — migration arrival rate (the parameter of Poisson distribution);

μ, σ^2 — mathematical expectation the variance of the relative number of elementary operations (parameters of normal distribution);

For post-copy migration lg$X$ should be taken instead of X.

3. Construct the time dependences of the parameters $\alpha(T)$, $\sigma(T)$ and $\lambda(T)$.

4. Using the method of least squares, find the values of the coefficients γ and β in the models.

$$\alpha(T) = \gamma_1 \cdot T(1 - e^{-\beta_1 x})$$

$$\lambda(T) = \gamma_2 \cdot T(1 - e^{-\beta_2 x})$$

$$\sigma^2(T) = \gamma_3 \cdot T(1 - e^{-\beta_3 x})$$

5. Find the ratios of the coefficients obtained

$$c_1 = \frac{\gamma_1}{\gamma_2}; \quad c_2 = \frac{\gamma_3}{\gamma_2};$$

6. Calculate b by formula

$$b = \frac{2\sqrt{c_2 - c_1^2}}{c_2}$$

7. Substitute the obtained coefficients in the expression for the distribution density of the migration total migration time.

The general algorithm of the method is shown in fig. 4. To simplify the calculations, it is proposed to use the Charlier A-series, which is acceptable for the studied volume of statistical data.

The obtained expression allows us to determine with certain probability the window closure criterion on the local controllers in the data center resource management system, which is important for effective system monitoring.

Conclusion

In this work the full cycle of works on the resource management of the infocommunication system of cloud data centers is proposed, including models and methods of initial and dynamic placement of virtual machines and horizontal scaling. It takes into account the VM live migration, which, in comparison with other models and methods, allows maintaining the stability and quality of cloud services for infocommunication system.

For forecasting it is proposed to use the group method of data handling, which allows to increase the accuracy of the server overload forecast, to reduce the number of unnecessary migrations and to increase the stability of the cloud data center as a whole.

A method for calculating the total migration time is proposed, based on finding an approximate analytical expression for the probability density, which makes it possible to determine with certain probability the window closure criterion on local controllers in the data center resource management system.

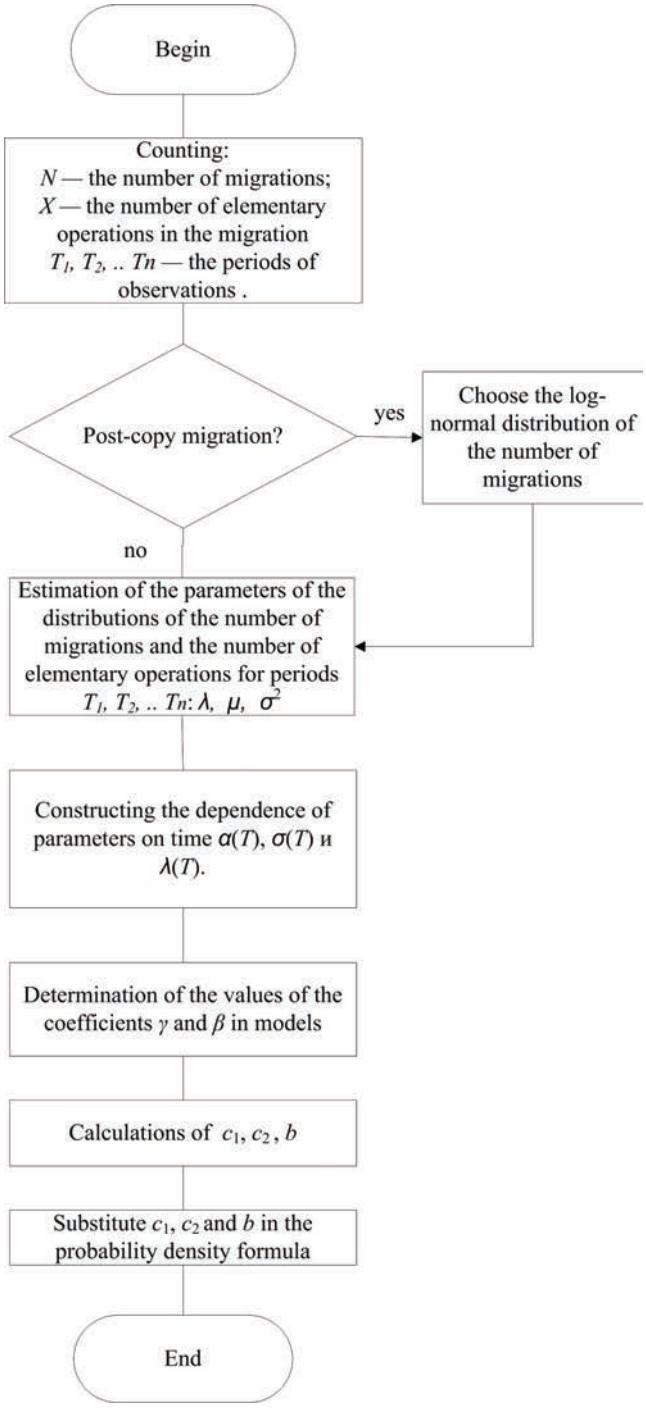


Fig. 4. The algorithm for obtaining the probability density of total migration time

References

1. Verma A., Ahuja P., Neogi A. pMapper: power and migration cost aware application placement in virtualized systems. *Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware (Leuven, Belgium, December 1–5, 2008)*. New York, 2008. Vol. 5346. Pp. 243–264.

2. Mikryukov A.A., Hantimirov R. Initial resource provisioningin iaas clouds based on the analytic hierarchy process. *Statistics and Economics*. 2015. No. 4. Pp.184–187. URL: https://doi.org/10.21686/2500–3925–2015–4–184–187. (In Russian)

3. Kostenko V.A., Plakunov A.V. Ant Algorithms for Scheduling Computations in Data Processing Centers. *Moscow University Computational Mathematics and Cybernetics*. 2017. Vol. 41. No.1. Pp. 44–50.

4. Alharbi F., Tian Y.C., Tang M., Ferdaus M.H. Profile-Based Ant Colony Optimization for Energy-Efficient Virtual Machine Placement. *Proc. of the International Conference on*

Neural Information Processing, ICONIP 2017(Guangzhou, China, November 14–18, 2017). In: Liu D., Xie S., Li Y., Zhao D., El-Alfy E.S.M. (eds). Springer, 2017. Vol. 10634. Pp. 863–871.

5. Xu J., Fortes J. Multi-objective Virtual Machine Placement in Virtualized Data Center Environments. *Proceedings of the Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom), Hangzhou, 18–20 December 2010*. IEEE, 2010. Pp. 179–188.

6. Vorozhtsov A. S., Tutova N. V., Tutov A. V. Optimal cloud servers placement in data centers. *T-Comm*. 2015. Vol. 9. No. 6. Pp. 4–8. (In Russian)

7. Vorozhtsov A. S., Tutova N. V., Tutov A. V. Dynamic computing resource allocation in data centers. *T-Comm*. 2016. Vol. 10. No.7. Pp. 47–51. (in Russian)

8. Beloglazov A., Buyya R. Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in Cloud data centers. *Concurrency and Computation: Practice and Experience (CCPE)*. 2012. Vol. 24. No. 13. Pp. 1397–1420.

9. Larin A. A., Abrosimov L. I. A Methodology for Redistributing the Operating Virtual Machines among the Servers in a Data Center. *Vestnik MEI*. No. 1. Pp. 98–105. DOI: 10.24160/1993–6982–2018–1–98–105. (In Russian)

10. Li X., Garraghan P., Jiang X. et al. Holistic Virtual Machine Scheduling in Cloud Datacenters towards Minimizing Total Energy. IEEE Transactions on Parallel and Distributed Systems. 2018. No. 29 (6). Pp. 1317–1331.

11. Radhakrishnan A., Kavitha V. Energy conservation in cloud data centers by minimizing virtual machines migration through artificial neural network. *Computing*. 2016. Vol. 98. Issue 11. Pp 1185–1202.

12. Vorojcov A. S., Tutova N. V., Tutov A. V. Performance evaluation of cloud data centers. *T-Comm*. 2014. Vol. 8. No. 5. Pp. 69–71. (In Russian)

13. Kaneko Y., Ito T., Ito M., Kawazoe H. Virtual Machine Scaling Method Considering Performance Fluctuation of Public Cloud. *2017 IEEE10th International Conference on Cloud Computing (CLOUD2014), Honolulu, 25–30 june 2017)*. NY, 2017. Pp. 782–785. doi: 10.1109/CLOUD.2017.114

14. Tikhomirov P. O., Emelyanov P. V., Plotnik N. S., Zyryanov A. V. Minimizing downtime processes during their migration in the cloud hosting. *Novosibirsk State University Journal of Information Technologies*. 2014. Vol. 12. No. 4. Pp. 112–120. ISSN1818–7900. (In Russian)

15. Akoush S., Sohan R., Rice A., Moore A. W., Hopper A. Predicting the performance of virtual machine migration. *18th IEEE/ACM International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems, MASCOTS2010 (Miami, Florida, USA, 2010)*. IEEE, 2010. Pp. 37– 46. DOI: 10.1109/MASCOTS.2010.13

16. Jo C., Cho Y., Egger B. A machine learning approach to live migration modeling. P*roceedings of the 2017 Symposium on Cloud Computing – SoCC'17 (Santa Clara, CA, USA, September 24–27, 2017)*. New York, 2017. Pp. 351–364. DOI:10.1145/3127479.3129262

17. Vorozhtsov A.S., Tutova N. V. Algorithm for solving optimization problems of resource allocation of data centers in the Internet. *T-Comm*. 2009. No. S2. Pp. 144–146. (In Russian)

18. Tutov A.V., Tutova N. V., Vorozhtsov A. S. Modeling of resource allocation in cloud data centers. *T-Comm*. 2017. Vol. 11. No.4. Pp. 76–80.

19. Buyya R., Ranjan R., Calheiros R. N. Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities. *Proc. of International Conference on High Performance Computing & Simulation (Leipzig, 21–24 June 2009)*. IEEE, 2009. Pp. 1–11. DOI: 10.1002/spe.995.

20. Clark C., Fraser K., Hand S., Hansen J. G., Jul E., Limpach C., Pratt I., Warfield A. Live migration of virtual machines. *Proceedings of the 2nd Symposium on Networked Systems Design & Implementation, NSDI'05 (Berkeley, CA, USA May 02–04, 2005)*. USENIX Association, 2005. Vol. 30. No. 4. Pp. 273–286.

21. Vorozhtsov A.V., Toutova N. V., Toutov A. V. Resource control system stability of mobile data centers. *2018 Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow 14–15 March 2018)*. IEEE, 2018. Pp. 1–4.

22. Tutov A. V. Resource control system of cloud datacenters. *Datchiki & Systemi* [Sensors & Systems]. 2018. No.7. Pp.15–20. (In Russian)

23. Legkov K. E. (2016). Models and methods of monitoring parameters characterizing the state of the infocommunication systems a special purpose. *T-Comm*. Vol. 10. No. 1. Pp. 11–18. (In Russian)

24. Baginyan A., Dolbilov A., Korenkov V. Equal cost multi pathing in high power systems with TRILL. *T-Comm*. 2017. Vol. 11. No. 4. Pp. 14–19. (In Russian)

25. Baginyan A., Dolbilov A., Korenkov V. Equal cost multi pathing in high power systems with TRILL. *T-Comm*. 2017. Vol. 11. No. 4. Pp. 14–19. (In Russian)

26. Dokuchaev V.A., Kalfa A.A., Mytenkov S. S., Shvedov A. V. Technical solutions analysis for the modern Data Centers. *T-Comm*. 2017. Vol. 11. No. 6. Pp. 16–24. (In Russian)

27. Goncharov A. M., Chashhin S. V., Prokhorov M. A. Approach to the solution of the problem of estimation of steady functioning of the information system on the example of data-processing centre. *T-Comm*. 2017. Vol. 11. No. 4. Pp. 20–25. (In Russian)

28. Vorozhtsov A. S., Tutova N. V., Tutov A. V. The technique of optimal virtual server placement in data centers. *T-Comm*. 2015. Vol. 9. No. 7. Pp. 5–10. (In Russian)

29. Abaev P. O., Razumchik R. V., Uglov I. V. Analysis of the SIP-traffic model of a contact center according to the treatment results of network measurements. *T-Comm*. 2013. Vol. 7. No. 11. Pp. 4–10. (In Russian)

30. Gudkova I.A., Maslovskaya N. D. A probable model for analysis of delays of access to the infrastructure of cloud calculations with a monitoring system. *T-Comm*. 2014. Vol. 8. No. 6. Pp. 13–15. (In Russian)

МОДЕЛИ И МЕТОДЫ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ ОБЛАЧНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

ТУТОВ АНДРЕЙ ВЛАДИМИРОВИЧ,
г. Москва, Россия, andrew_vidnoe@mail.ru

КЛЮЧЕВЫЕ СЛОВА: управление ресурсами; облачные технологии; размещение виртуальных машин; живая миграция; центр обработки данных.

АННОТАЦИЯ

Основной проблемой современных центров обработки данных является потребление колоссальных объемов электроэнергии, значительная часть которой идет на инфокоммуникационную систему и систему охлаждения, которая начинает усиленно работать в случае неравномерного распределения температуры в зале. Поэтому необходимо совершенствовать методы распределения ресурсов для минимизации энергопотребления, при этом обеспечивая высокий уровень качества сервисов. Перераспределение ресурсов в облачном центре обработки данных происходит путем живой миграции виртуальных машин, которая дополнительно нагружает систему и мешает осуществлять мониторинг серверов. Данный факт учитывать в процессе управления. В настоящее время существует большое количество работ, посвященных отдельным вопросам оптимального распределения и управления ресурсами облачных центров обработки данных. Однако в известных работах отсутствует полный цикл работ. В данной работе предложены модели и методы полного цикла работ по оптимизации и управлению ресурсами инфокоммуникационной системы облачного центра обработки данных. В частности, предложена модель первоначального размещения виртуальных машин в виде задачи многокритериальной оптимизации и метод ее решения. Приведена двухуровневая система управления ресурсами, которая включает в себя локальные и глобальный контроллер. Локальный контроллер осуществляет мониторинг загрузки и температуры серверов и делает прогноз на следующее окно наблюдения. Для прогнозирования предложено использовать метод группового учета аргументов. Для определения размера окна наблюдения необходимо учитывать длительность миграции. Проведено исследование двух видов живой миграции и предложен метод расчета длительности живой миграции, на основе нахождения аналитического выражения плотности вероятности, позволяющего с определенной вероятностью определить критерий закрытия окна на локальных контроллерах в системе управления ресурсами центров обработки данных. Для сервисов SaaS и PaaS, использующих горизонтальное масштабирование, предложена модель двухкритериальной оптимизации числа виртуальных машин в кластерах крупного многозвенного приложения, которую предложено решать комбинированным методом последовательных уступок и ограничений.

СВЕДЕНИЯ ОБ АВТОРЕ:

Тутов А.В., старший преподаватель Московского технического университета связи и информатики.

Для цитирования: Тутов А.В. Модели и методы распределения ресурсов инфокоммуникационной системы облачных центров обработки данных // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 100–107. doi: 10.24411/2409-5419-2018-10192 (Англ.)

ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

Редакция журнала H&ES Research принимает к публикации статьи на русском и английском языках. Предоставляемая рукопись должна быть актуальной, обладать новизной, отражать постановку задачи, содержать описание основных результатов исследования, выводы, а также соответствовать указанным ниже правилам оформления. Текст должен быть тщательно вычитан автором, который несет ответственность за научнотеоретический уровень публикуемого материала.

Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, аннотация, ключевые слова, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями рисунков в формате TIFF, EPS по требованиям указанным в п.7.

К статье прилагается экспертное заключение о возможности опубликования статьи в открытой печати и две рецензии кандидатов или докторов наук по профилю планируемой публикации материалов (сканированные копии в электронном виде).

Все материалы высылаются электронной почтой в адрес журнала: HT-ESResearch@yandex.ru.

1. **Статья подготавливается** в редакторе MS Word. Шаблон статьи можно скачать на сайте журнала www.h-es.ru.

2. **Данные об авторе:** фамилия, имя, отчество, ученая степень, звание, должность и полное название организации – места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.

3. **Объем аннотации** 200–250 слов. Аннотация должна быть информативной (не содержать общих слов), без сокращений, структурированной, отражать основное содержание статьи: предмет, цель, методологию проведения исследований, результаты исследований, область их применения, выводы. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье. Предложения должны начинаться словами: показано, получено, исследовано, предсказано и т.д. и т.п.

4. **Ключевые слова:** от 5 до 7 слов (словосочетаний), разделенных точкой с запятой.

5. **Объём статьи** без аннотации – от 15 до 30 тыс. знаков с пробелами. Рисунки и таблицы в объеме статьи не учитываются.

6. **Формульные выражения** выполняются в редакторе Math Type. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается. Длина формулы в одну строчку 8–9 см.

Простые формулы и буквенные обозначения величин следует писать в строку обычным текстом. В формулах использовать только буквы латинского и греческого алфавита!

Размеры шрифтов (Size) предварительно перед набором первой формулы установить (в MathType) следующие: кегль основной – 10, крупный индекс – 7, мелкий индекс – 5, крупный символ – 12, мелкий символ – 8. Формулы, не содержащие специальных математических символов, должны быть набраны в тексте (в формате Word). Греческие обозначения, скобки (квадратные и круглые) и цифры всегда набираются прямым шрифтом. Латинские буквы набираются курсивом как в формулах, так и в тексте, кроме устойчивых форм (max, min, cos, sin, tg, log, exp, det …).

Нельзя использовать сканированные формулы! Все формулы должны быть набраны вручную!

7. **Рисунки и таблицы** в статье должны быть пронумерованы и снабжены подписями, в тексте статьи должны иметься ссылки на каждый рисунок и таблицу (рис.1 и табл.1). Если рисунок или таблица единственные в статье, то их не нумеруют.

Рисунки должны быть четкими, с хорошо проработанными деталями. Избегать текстовых надписей на иллюстрациях. Заменять их цифровыми обозначениями, которые поясняются в подписи или в основном тексте. Все рисунки прилагаются в виде отдельных файлов в формате TIFF, EPS с разрешением не менее 300 dpi для оригинального размера в печатном издании (для больших рисунков ширина от 14 до 20 см, для маленьких от 7 до 9 см).

8. **Список литературы:** от 15 до 50 наименований. Из них самоцитирований не должно быть более 25%. В числе источников желательно не менее 50 % иностранных источников (для статей на английском языке – 15% российских). Состав источников должен быть актуальным и содержать не менее 8 статей из научных журналов не старше 10 лет, из них 4 – не старше 3 лет.

Ссылки должны быть только на статьи, патенты, книги и статьи из сборников трудов. В списках литературы не размещать ГОСТЫ, рекомендации, диссертации, авторефераты и другую нормативную и непериодическую документацию. Эти данные можно указывать в теле статьи в скобках или в виде постраничных сносок (если автор непременно хочет указать нормативный документ или сослаться на свою диссертацию). Список литературы оформляется в соответствии с ГОСТ 7.052008. **Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.**

9. **На английском языке** предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Все названия издательств и журналов должны быть транслитерированы, а не переведены. Названия организаций в списках литературы (Труды Академии...) должны быть четко выверены с данными организации и иметь официальное английское наименование, которое указано на их сайте или также транслитерированы. Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.

10. **Структура статьи на английском языке**

Introduction (введение)

Materials and methods (материалы и методы).

Results and Discussions (результаты и обсуждение).

Conclusions (вывод)

Acknowledgements (благодарности, необязательный раздел)

References (ссылки на использованную литературу)

На руском языке предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Внимание! Редакция оставляет за собой право отклонить представленные материалы, оформленные не по указанным правилам.