
СПЕЦВЫПУСК
**S2-2016**

Издается с 2009 года
Издательская лицензия ПИ № ФС 77-60899
Язык публикаций: русский, английский
Периодичность выхода – 6 номеров в год
Сайт в Интернете: www.H-ES.ru
E-mail: **HT-ESResearch@yandex.ru**

УЧРЕДИТЕЛЬ:
ООО «Издательский дом Медиа Паблишер»

ГЛАВНЫЙ РЕДАКТОР:
Константин Легков

ИЗДАТЕЛЬ:
Светлана Дымкова

ПРЕДПЕЧАТНАЯ ПОДГОТОВКА:
ООО «H&ES Research»

АДРЕС РЕДАКЦИИ:

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

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

Журнал H&ES Research зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.
Мнения авторов не всегда совпадают с точкой зрения редакции. За содержание рекламных материалов редакция ответственности не несет.


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.**



**H&ES Research** – один из ведущих рецензируемых научных журналов, в котором публикуются основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук. Журнал 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.
Научно-технический журнал **H&ES Research** предназначен прежде всего для специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств космических исследований Земли и информационной безопасности. В журнале публикуются новости о событиях в вышеуказанных областях, репортажи и интервью ведущих компаний, мнения специалистов, новые технологии, инновационные разработки, оборудование и решения, аналитические статьи, маркетинговые исследования и др.

**Журнал H&ES Research входит в Перечень ВАК** и в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий **ISSN 2412-1363 (Online), 2409-5419 (Print).**

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:
- 01.01.00 Математика
- 05.07.00 Авиационная и ракетно-космическая техника
- 05.11.00 Приборостроение, метрология и информационно-измерительные приборы и системы
- 05.12.00 Радиотехника и связь
- 05.13.00 Информатика, вычислительная техника и управление

**ТЕМАТИЧЕСКИЕ НАПРАВЛЕНИЯ**

- Вопросы развития автоматизированных систем управления
- Физико-математическое обеспечение разработки новых технологий
- Развитие автоматизированных систем управления технологическим процессом
- Вопросы исследования космоса
- Телекоммуникационные технологии и технические новинки систем подвижной связи
- Перспективы развития единого инфокоммуникационного пространства
- Использование радиочастотного спектра в системах подвижной связи
- Антенно-фидерное оборудование
- Спутниковое телевидение, системы спутниковой навигации, GLONASS, построение навигационных систем GPS
- Вопросы развития геодезии и картографии
- Информационная и кибербезопасность
- Вопросы исследования Арктики
- Волоконно-оптическое оборудование и технологии
- Метрологическое обеспечение
- Программное обеспечение и элементная база для сетей связи
- Производители, поставщики и дистрибьюторы телекоммуникационного оборудования
- Работа отечественных ассоциаций, региональных и координирующих операторов
- Правовое регулирование инфокоммуникаций, законодательство в области связи
- Экономика связи, конвергенция сетей, универсальные коммуникации
- Выставки, форумы, конференции, семинары, интервью (оригинальные и новые проекты, итоги деятельности, проблемы отрасли и пути их решения и т.д.)

**РЕДАКЦИОННАЯ КОЛЛЕГИЯ**



Отдел развития и рекламы: Ольга Дорошкевич, ovd@media-publisher.ru, тел.: 8(916) 951-55-36.

**H&ES Research** – one of leading reviewed scientific journal in whom the main scientific results of the dissertation on competition of a scientific degree of the doctor and the candidate of science are published. 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.
**H&ES Research** – journal for specialists in the field of modern information and communication technologies and automated systems management means for Space Research of the Earth and information security. The journal publishes news about events in the above areas, reports and interviews of the leading companies, the opinions of experts, new technologies, innovations, products and solutions, analytical articles, market research and others.

The journal 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:
• 01.01.00 Mathematics
• 05.07.00 Aviation, space-rocket hardware
• 05.11.00 Instrument engineering, metrology and information-measuring devices and systems
• 05.12.00 RF technology and communication
• 05.13.00 Informatics, computer engineering and control

**TOPICAL COLUMNS**

• Automated control systems
• Physical and mathematical software development of new technologies
• Development of automated process control systems
• Questions of space exploration
• Telecommunication technology and technical innovations of mobile systems
• Prospects for unified info communication space
• Use of a radio-frequency range in systems of mobile communication
• Antenna-feeder equipment
• Satellite TV, satellite navigation system, GLONASS, GPS navigation systems construction
• Issues of Geodesy and Cartography
• Information and cyber security
• Questions Arctic research
• Fiber-optic equipment and technology
• Metrological maintenance
• Software and electronic components for communication networks
• Manufacturers, suppliers and distributors of telecommunications equipment
• National associations, regional and coordinating operators
• Legal regulation of Infocomm, legislation in the communication field
• Economy of communications, networks convergence, universal communication
• Exhibitions, forums, conferences, seminars, interview (original and new projects, results of activity, a problem of branch and a way of their decision, etc.)



Development and advertizing department: Olga Doroshkevich, ovd@media-publisher.ru, tel.: 8(916) 951-55-36.

H&ES RESEARCH

SPECIAL ISSUE
**S2-2016**

It is published since 2009
Publishing license ПИ № ФС 77-60899
Language of publications:
Russian, English
Periodicity – 6 issues per year
Site on the Internet: www.H-ES.ru
E-mail: **HT-ESResearch@yandex.ru**

FOUNDER: «Media Publisher», LLC

EDITOR IN CHIEF: Konstantin Legkov

PUBLISHER: Svetlana Dymkova

PREPRESS: «H&ES Research», JSC

ADDRESS OF EDITION:
111024, Russia, Moscow,
st. Aviamotornaya, 8, office 512-514

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

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. The opinions of the authors don't always coincide with the point of view of the publisher. For the content of ads, the editorial Board is not responsible.


GRADUATE 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.



**«H&ES RESEARCH – HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH» JOURNAL**

WWW.H-ES.RU

HES_Research HES-Research
club55425245

# НПЦ ИРС

Научно-производственный центр
Информационных региональных систем

▸ npcirs.ru

Закрытое акционерное общество "Научно-производственный центр информационных региональных систем" является предприятием, разрабатывающим автоматизированные системы специального назначения.

## Основными направлениями нашей деятельности являются:

- проектирование, создание и ремонт автоматизированных систем управления и их составных частей, систем обработки данных, программного обеспечения, информационных систем для государственных организаций и коммерческих компаний;
- разработка общесистемного и прикладного ПО, внедрение и сопровождение информационных систем;
- защита информации в системах управления, локальных вычислительных сетях, программно-аппаратных комплексах, телекоммуникационных системах;
- производство и поставка технических средств, в офисном и защищенном исполнении;
- создание, внедрение и сопровождение оперативных и учетных систем любой сложности;
- анализ автоматизированных систем на предмет разработки к ним классификаторов и нормативно-справочной информации;
- разработка проектов и создание глобальных, корпоративных, локальных телекоммуникационных систем и структурированных кабельных сетей.

Создаваемые предприятием средства (комплексы средств автоматизации, программные и программно-информационные комплексы, информационные изделия) эксплуатируются в различных государственных органах: в органах военного управления Министерства обороны РФ, а также на предприятиях, в организациях, в органах местного самоуправления субъектов РФ, занимающихся воинским учетом.
Научные исследования в сфере КНСИ позволяют нам качественно анализировать автоматизированные системы и разрабатывать к ним классификаторы и нормативно-справочную информацию.

## На данный момент уже имеющиеся разработки позволяют:

- создавать классификаторы по единым правилам, независимо от их содержимого;
- создавать массивы классификационной, нормативно-справочной информации в виде эталонных и контрольных экземпляров;
- создавать и вести централизованный банк УММ классификаторов (нормативные документы кодирования сведений);
- комплектовать массивы КНСИ для поставки на объекты, в части касающейся;
- проводить учет КНСИ и поставку на объекты автоматизации;
- централизованно вносить изменения в КНСИ;
- синхронизировать взаимодействие объектов, использующих классификаторы (КНСИ) и УФД;
- обеспечить совместимость данных баз данных объектов;
- обеспечить обмен базами данных между различными автоматизированными системами с территориально разнесенными источниками информации.

Коллектив ЗАО "НПЦ ИРС" образован на основе коллектива Государственного унитарного предприятия. Унаследовав его опыт научно-производственной деятельности, профессиональные знания коллектива специалистов, который целенаправленно занимается проблематикой автоматизации деятельности должностных лиц органов военного управления Вооруженных Сил РФ и разработкой единого информационного обеспечения автоматизированных систем военного назначения более 15 лет, выполняя как теоретические, так и практические работы в этой области.

НПЦ ИРС
Научно-производственный центр
Информационных региональных систем
▸ npcirs.ru

Телефон: 8(800)100-40-90
E-mail: administrator@npcirs.ru

# СОДЕРЖАНИЕ

# CONTENTS

# АНАЛИЗ МЕТОДОВ РАСПРЕДЕЛЕНИЯ ПОТОКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Оркин Вадим Витальевич,**
*адъюнкт Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия*

**Левко Игорь Владимирович,**
*к.т.н., доцент Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия*

**Умаров Александр Бахтиерович,**
*курсант Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия*

**Аннотация**

Работа посвящена исследованию проблем распределения потоков заявок на предоставление информационных услуг в информационных подсистемах автоматизированных систем управления специального назначения. Информационная подсистема включает в себя информационные системы пунктов управления и комплексов средств автоматизации автоматизированных систем управления. Функциями информационной подсистемы являются: управление коммутацией, передачей, предоставление информации, управление услугами.

Одной из задач управления информационными подсистемами специального назначения является обеспечение процедур направления потоков заявок на предоставление информационных услуг по путям, проходящим через вполне конкретные узлы предоставления услуг данных систем. Существует план распределения потоков заявок. Он представляет собой совокупность таблиц маршрутизации всех узлов информационной подсистемы и определяет заданную на определённое время очерёдность выбора исходящих направлений передачи из каждого узла предоставления услуг ко всем остальным узлам. На первом историческом этапе построения информационных систем и сетей заранее спланированные пути передачи информации задавались при проектировании этих систем и сетей. Задача выбора путей передачи заявок и сообщений не являлась одной из подзадач управления сетью. Однако позднее появилось понятие «динамическое управление сетью», предполагающее постановку задачи формирования и выбора маршрутов в сети как задачу управления.

Динамическое управление сетью предполагает адаптивную маршрутизацию. Под адаптивностью будем понимать такое функционирование системы, которое изменяется с учётом состояния внешней среды и внутреннего состояния, что определяет маршруты доставки в соответствии с этими состояниями. Динамические алгоритмы управления сетью принимают во внимание не только структуру самой сети, но и требования, предъявляемые к процессу передачи сообщений. Эффективность адаптивной маршрутизации информационной подсистемы зависит от правильной информации о состоянии подсистемы и поступающих потоков пакетов данных.

**Ключевые слова:** *информационная подсистема, распределение потоков, маршрутизация, автоматизированная система управления, эффективность.*

**Введение**

Эффективность информационной подсистемы специального назначения (ИПС СН) во многом определяется используемыми протоколами маршрутизации и методами управления потоками заявок на предоставление услуг. Исходя из этого, вопросы организации процедур распределения потоков заявок в ИПС СН являются весьма важными и определяющими эффективность функционирования ИПС СН.

В настоящее время в той или иной мере стандартизировано достаточно много протоколов маршрутизации, ряд из которых широко применяется в информационных системах и сетях (ИС) [1-3]. Однако использование стандартных решений и протоколов не всегда оправдано в ИПС СН в связи с особенностью условий функционирования данных систем, а сведение управления потоками заявок к минимально требуемому уровню не желательно, исходя из важности решаемых задач органами управления, в которых эти системы функционируют. Поэтому представляется целесообразным провести анализ методов управления потоками заявок на предоставление услуг в информационных системах на предмет возможности их применения в ИПС СН с условием обеспечения необходимого уровня качества обслуживания.

**Анализ существующих методов распределения потоков в информационных системах и сетях**

Изначально появились статические детерминированные методы формирования плана распределения информационных потоков. Согласно данным методам порядок выбора исходящего направления передачи для всех узлов задан заранее и не изменяется с течением времени. В случае попытки передачи заявки на получение услуги по направлению, определённому в таблице маршрутизации приоритетным, но занятому в этот самый момент, происходит выбор второго по приоритету направления. Но данный выбор может быть неоправданным в случае, если занятие пути первого выбора было кратковременным. Существенные же изменения в структуре ИС могут привести к ситуации, когда составление плана распределения окажется за пределами возможностей этого метода, т.е. реально информацию можно передать по какому-нибудь существующему пути, но в матрице маршрутизации его просто не существует. Эффективность применения статического детерминированного группового метода для ИС СН достаточна низкая, так как в условиях изменения внешних условий может измениться как интенсивность потоков заявок в системе, так и структура системы (выход из строя узлов, ветвей); также возможна перегрузка направлений и сбои сетевых элементов. Тем не менее, статические детерминированные групповые (для всех заявок в определённом интервале времени) методы управления потоками всё еще применяются в ИС СН, так как введение центров адаптивного управления видится неоправданным для руководящего состава. Это справедливо и экономически оправдано только в случае, когда потоки заявок на предоставление услуг равномерны и нет внешнего воздействия на ИС СН и её структуру.

Вариантом усовершенствования статических методов распределения потоков является квазистатический метод [4, 6]. Направления совершенствования существующего статического метода показаны на рис. 1.

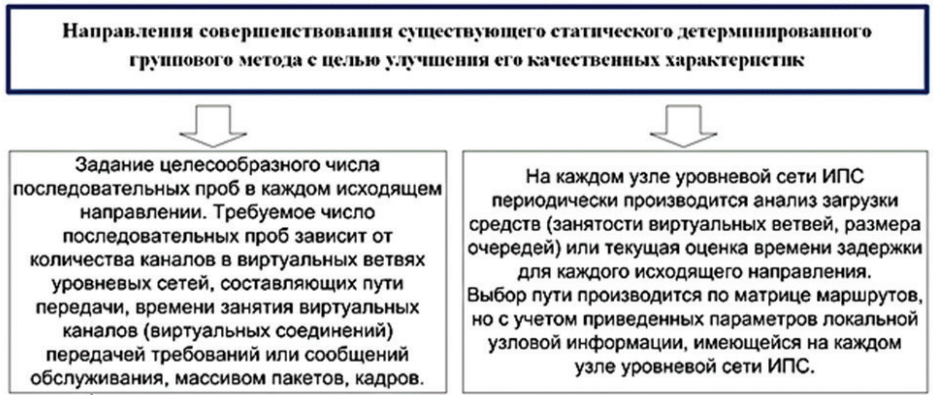



**Рис. 1**. Направления совершенствования существующего статического метода

Первое направление связано с заданием целесообразного числа последовательных проб в каждом исходящем направлении. При неудачной попытке передать пакет или установить соединение по пути первого выбора полезно предпринять еще несколько попыток, прежде чем переходить к выбору следующего пути. Требуемое число последовательных проб зависит от количества направлений в ветвях, составляющих путь, и времени занятия виртуальных соединений передачей сообщения [6]. За целесообразное число проб можно взять величину $\frac{\gamma \bar{t}_з}{m\Delta t}$, где $\bar{t}_з$ — время занятия соединения передачей сообщения (заявки), $m$ — число каналов в ветви, $\Delta t$ — интервал времени между двумя последовательными попытками передать сообщение, $\gamma$ — весовой коэффициент, характеризующий различия между путём первого и второго (третьего) выбора [6] (рис. 2). Недостатком данного квазистатического метода распределения потоков является затрачивание времени на проверку тракта, который не может быть построен из-за выхода из строя направлений передачи информации.

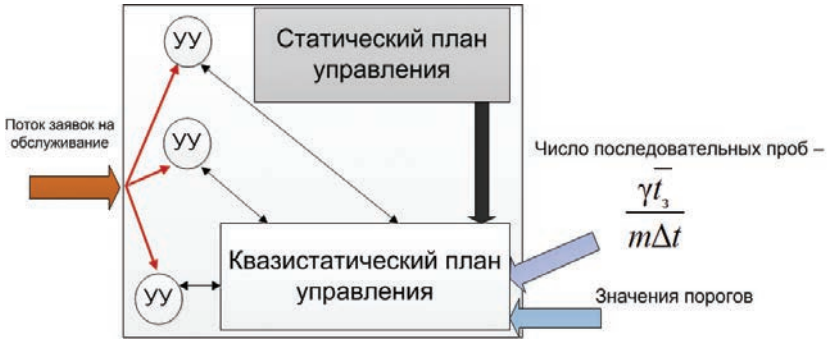



**Рис. 2**. Описание квазистатического метода распределения потоков

Второе направление связано с частичным введением адаптивного управления, которое связано с анализом локальной информации о загруженности исходящих путей передачи либо о времени задержек и длинах очередей. Выбирается путь, который на исходящем направлении менее загружен, характеризуется меньшей задержкой. Если пути первого, второго и.т.д. выбора различ-

ны по длине, то процедура выбора усложняется введением ограничений. Требуется задание значений порогов для путей различного выбора, которое должно быть произведено заранее путём моделирования функционирования сети. Таким образом, сообщение посылается по второму направлению, когда первое направление загружено на определённую величину.

Данная модернизация значительно улучшает статические методы и может повысить эффективность ИС СН при тщательном и регулярном подборе и изменении параметров (время между последовательными пробами, их число, веса направлений при выборе маршрута передачи заявок).

Основным недостатком для второго направления развития квазистатического методов является отсутствие на узлах информации о наличии участков с большой загрузкой (отсутствием загрузки) на всем тракте передачи.

Устранён данный недостаток в так называемом «лавинном» методе. «Лавинный» метод формирования плана распределения информации (в отечественной литературе известен как «Волновой») на ИС состоит в следующем. В каждом узле коммутации через определённое время $\Delta t = \text{const}$ формируются зонд-сигналы, которые пересылаются ко всем инцидентным узлам [5]. Данные сигналы попадают во все узлы ИС и анализируют по мере продвижения вероятностно-временные характеристики всех элементов ИС СН. Для сетей с дейтаграммной передачей пакетов в качестве сигналов поисковой волны служат сами информационные пакеты.

Лавинный метод реализован в технологии ATM и IP всех версий. Недостатком данного метода является повышение загруженности ИС в результате передачи потоков зонд-сигналов, что может сократить вероятность своевременного обслуживания заявок на предоставление услуг в ИС СН во время функционирования системы в режиме повышенной нагрузки. Преимуществом является то, что на каждом узле имеется актуальная информация об изменении структуры ИС либо на время установления одного соединения, либо (при групповом обслуживании) с созданием таблиц маршрутизации.

В других источниках лавинный метод является разновидностью волновых методов применительно к ИС с дейтаграммной передачей пакетов.

Применение данного метода эффективно при групповом обслуживании заявок, когда волны организуются через относительно большой промежуток времени (в целях предотвращения загруженности ИС). План распределения потоков таким образом периодически корректируется. В паре с таким методом распределения может быть применён первый из вышеупомянутых квазистатических методов с сокращением числа последовательных проб для снижения времени передачи запроса к серверу.

Статистический (игровой) метод распределения потоков предусматривает формирование плана распределения по статистическим данным, накопленным за определённое время эксплуатации ИС. Таблице маршрутизации ставится в соответствие таблица весовых коэффициентов, представляющих собой вероятности передачи сообщения по определённому маршруту (от *j*-го узла к *i*-му). В итоге на каждом узле формируется матрица весовых коэффициентов. При поиске маршрута к *i*-му узлу происходит обращение к *i*-м строкам матриц маршрутизации (матриц весовых коэффициентов) узлов передачи, в которых находится максимальный весовой коэффициент, соответствующий определённому маршруту. В результате маршрут между заданной парой узлов будет или определён, или данное требование получит отказ. В первом случае маршрут поощряется (весовой коэффициент увеличивается по определённому алгоритму), а в противном случае штрафуется (весовой коэффициент уменьшается). Элементы матрицы коэффициентов нормируются. Таким образом, формируется оптимальный план распределения потоков по критерию результата установления соединения в предыдущий период.

Одним из вариантов статистических методов является вероятностно-игровой метод распределения потоков [4, 6]. Вначале наугад выбирается исходящее направление. Если виртуальное соединение установлено или передача информации успешно завершена, то направление поощряется, в противном случае штрафуется. Через некоторое время накопится статистика успешных и неуспешных соединений или передач пакетов, и выбор будет осуществляться осознанно.

Основное преимущество статистического метода заключается в том, что при формировании плана распределения потоков заявок не требует передачи по ИС какой-либо служебной информации. Недостатком данного метода является его


**Рис. 3**. Алгоритм вероятностно-игрового метода управления потоками

большая инерционность. При изменении структуры ИС требуется большой промежуток времени для изменения матрицы весовых коэффициентов и достижения её адекватности. Реакция на структурные изменения в сети существенно возрастает при возможности своевременного централизованного изменения таблиц маршрутизации, однако, накопленная статистика при этом должна фактически обнулиться, т.е. после структурного изменения в ИС статистику придется набирать заново. Поэтому применение статистического метода нецелесообразно в ИС СН, в которых вероятность изменения структуры сети (в результате внешних воздействий) достаточно велика.

Централизованные методы изменения маршрутной информации подразумевают вычисление её параметров в одном центре управления. Но основным недостатком их является вероятность отличия информации о структуре ИС, имеющейся в центре управления от реального состояния. Информация об изменениях в ИС СН всегда приходит в центр управления ИС с задержкой, поэтому без локальной информации и адаптивного распределения потоков, осуществляемого отдельными узлами в данных ИС, не обойтись. Централизованное управление должно быть сведено большим образом к мониторингу изменений в ИС и возможности изменить локальную информацию на узлах без ущерба производительности при значительных структурных изменениях, к поддержке адаптивных децентрализованных методов распределения потоков.

**Анализ возможной реализации комбинированных методов распределения потоков в ИС СН**

Наиболее эффективным при выполнении задачи распределения потоков заявок на предоставление услуг в ИПС СН является применение комбинации как вышеперечисленных, так и других методов, выполняемых в зависимости от состояния системы, а также от состояния внешней среды.

Наряду с квазистатическими методами могут применяться волновые методы и разработанные на их основе специальные методы зондирования для определения новой структуры ИПС после различных воздействий. Причём применение лавинных методов, а также многих других методов, относящихся к классу волновых, может осуществляться не по всем направлениям, а лишь по наиболее предпочтительным. Выбор направления может быть осуществлен по геометрическому принципу (выбираются исходящие направления, близкие к прямой между узлами источника и получателя) или по принципу выбора направлений, отвечающих требуемому качеству обслуживания.

Возможна комбинация лавинного метода и статистического. В условиях отсутствия внешних деструктивных воздействий на элементы ИПС формирование плана распределения осуществляется статистическим методом. В условиях резкого изменения структуры ИПС применяются различные разновидности волновых методов распределения потоков.

**Выводы**

В результате проведённого в статье анализа методов распределения потоков заявок на предоставление услуг в ИПС АСУ СН определено, что применение статических методов распределения для системы, функционирующей в условиях изменяющейся обстановки неприемлемо. Применение динамических методов в ИПС АСУ СН должно быть обосновано современными требованиями, предъявляемыми к данным системам. Наиболее перспективным для повышения результативности ИПС АСУ СН видится комбинирование существующих методов в зависимости от её состояния. Применение выбранных для конкретной системы методов должно осуществляться по определённому алгоритму. Алгоритм адаптивного распределения потоков заявок на предоставление услуг должен работать на основе информации, полученной из баз данных, отражающих возможные состояния элементов и самой системы. Данная информация является как накопленной статистической, так и полученной в результате имитационного моделирования на средствах вычислительной техники. Данный алгоритм является основой методики обеспечения требуемых значений показателей эффективности функционирования ИПС АСУ СН.

**Список литературы**

1. *Лазарев В.Г.* Электронная коммутация и управление в узлах связи. М.: Связь, 1974, 271 с.

2. *Лазарев В.Г., Саввин Н.Г.* Сети связи, управление, коммутация. М.: Связь, 1973. 264 с.

3. *Буренин А.Н.* Об управлении маршрутизацией на основе модифицированных адаптивных методов // Техника средств связи. 1991. № 7. С.51–59.

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

5. *Новиков С.Н.* Классификация методов маршрутизации в мультисервисных сетях связи // Вестник СибГУТИ. 2013. № 1.

6. *Легков К.Е.* Методы управления параметрами, характеризующими процессы функционирования инфокоммуникационной системы специального назначения // T-Comm: Телекоммуникации и транспорт. 2016. Том 10. № 3. С. 49–55.

7. *Легков К.Е., Буренин А.Н.* К вопросу управления эффективностью инфокоммуникационных систем специального назначения // H&ES: Наукоемкие технологии в космических исследованиях Земли. 2014. Т. 6. 1. С. 38–43.

8. *Легков К.Е., Буренин А.Н.* Управление эффективностью инфокоммуникационных систем специального назначения // T-Comm: Телекоммуникации и транспорт. 2014. Том 8. № 3. С. 42–46.

## ANALYSIS OF METHODS OF FLOW DISTRIBUTION IN INFORMATION SYSTEMS FOR SPECIAL PURPOSES

**Orkin Vadim Vitalyevich,**
St. Petersburg, Russia, orc225@mail.ru

**Levko Igor Vladimirovich,**
St. Petersburg, Russia, levko_iv@mail.ru

**Umarov Aleksandr Bahtierovich**
St. Petersburg, Russia

**Abstract**
The work is devoted to research of flow distribution problems in the provision of information services for information subsystems of automated control systems for special purposes. Information subsystem includes information systems of control centers and complexes of automation means. The functions of the information subsystem are management of switching, transmission control, data providing management of services.
One of the tasks of information subsystem special purpose management is providing of procedures for the direction of flows of requests for information services to the ways passing through specific nodes of services of these systems. There is a plan for the distribution of requests flows. It is a set of routing tables of all nodes of information subsystem and it defines the order of the choice of the outgoing transmission lines from each node to provide service to all other nodes.
In the first stage of history of information systems and networks, pre-planned ways of data transmitting set during the process of design of these systems and networks. Selection task of transmission routes of requests and messages was not a subtask of network management. Later, however, the notion of "dynamic management of the network" appeared suggesting raising the problem of formation and selection of routes in the network as a management task.
Dynamic network management involves adaptive routing. We will understand the adaptability as a functioning of this system, which varies taking into account the state of the external environment and internal state that determines the delivery routes in accordance with these conditions. Dynamic network management algorithms take into account not only the structure of the network itself, but also the requirements for message transfer process. Efficiency of adaptive routing in information subsystem depends on correct information about the state of subsystem and incoming flows of data packets.
**Keywords:** information subsystem, flow distribution, routing.

**References**
1. Lazarev V. G. *Elektronnaya kommutaciya I upravlenie v uzlah svyazi* [Electronic switching and control nodes in the communication]. Moscow. Svyaz, 1974. 271 p. (in Russian)
2. Lazarev V. G. Savvin N. G. *Seti svyazi, upravlenie, kommutaciya* [Network communication, management, switching]. Moscow. Svyaz, 1973. 264 p. (in Russian)
3. Burenin A. N. About the routing control on the basis of modified adaptive methods. *Technique of communication*. 1991. No. 7. Pp. 51–59. (in Russian)
4. Burenin A. N., Legkov K. E. *Sovremennye infokommunikatsionnye sistemy i seti. Osnovy postroeniya i upravleniya transliteratsiya nuzhna* [Modern infocommunication systems and networks. Fundamentals of construction and management]. Moscow, Media Publisher Publ., 2015. 348 p. (In Russian).
5. Novikov S. N. Classification of routing methods in multiservice communication networks. *Vestnik SibGUTI*. 2013. No. 1. Pp. 57–67. (in Russian)
6. Legkov K. E. Methods of control of parameters characterizing the processes of functioning of the information systems of a special purpose. *T-Comm*. 2016. Vol. 10, No. 3. Pp. 49–55. (in Russian)
7. Legkov K. E. Burenin A. N. Control efficiency of the infocommunication systems of a special purpose. *H&ES Research*. 2014. Vol. 6. No. 1. Pp. 38–43. (in Russian)
8 Legkov K. E. Burenin A. N. Management efficiency of the infocommunication systems of a special purpose. *T-Comm*. 2014. Vol. 8. No. 3. Pp. 42–46. (in Russian)

**Information about authors:**
Orkin V. V., postgraduate student of the Department of automated systems of control, Military Space Academy.
Levko I. V., Ph.D., associate professor of the Department of automated systems of control, Military Space Academy.
Umarov A. B., military student of the Department of automated systems of control, Military Space Academy.

# ВОЗМОЖНОСТИ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОВЕДЕНИЯ РАСЧЁТНО-ОЦЕНОЧНОЙ ЭКСПЕРТИЗЫ ЭЛЕКТРОМАГНИТНОЙ СТОЙКОСТИ КОРАБЕЛЬНЫХ РЭС

**Биктеева Анастасия Максимовна,**
*инженер-программист 3 категории Центрального научно-исследовательского института «Курс», г.Москва, Россия, nbikteeva@gmail.com*

**Аннотация**
Рассматривается вопрос о возможности решения проблемы обеспечения защиты радиоэлектронных средств на морских объектах от преднамеренных электромагнитных воздействий. В качестве инструмента решения данной проблемы предлагается использование разработанного автором специализированного исследовательского программного комплекса на основе расчетно-оценочной экспертизы электромагнитной стойкости корабельных радиоэлектронных систем к преднамеренным силовым электромагнитным воздействиям, как инструмент информационной поддержки принятия решений по обеспечению заданного уровня радиоэлектронной защиты. Концепция, положенная в основу данного программного обеспечения, подразумевает то, что в зависимости от совокупности факторов электромагнитное воздействие может приводить к информационному, функциональному или физическому ущербу радиоэлектронной системы, и рассматривает взаимодействие источника электромагнитного излучения и устройства-рецептора как последовательность из восьми различных уровней электромагнитного взаимодействия: сигнального, фидерного и антенного контура источника, траекторного контура, антенного, фидерного, защитного и компонентного контура рецептора, для каждого из которых разработано расчётное численно-аналитическое методическое обеспечение. В результате расчетов предполагается выставление оценки электромагнитного поражения по семибалльной шкале, где 0 – нет влияния, 1 – слабая помеха, 2 – средняя помеха, 3 – одиночный сбой, 4 – многократный сбой, 5 – блокировка, 6 – прожиг. Подробно рассмотрен ход работы в программном комплексе в двух режимах: графическом, учитывающем двухмерное расположение множества антенн источников и рецепторов и позволяющем сформировать сводную таблицу результатов расчетов, и ручном, позволяющем проводить более подробное исследование для конкретной пары источник-рецептор. Рассмотрены ключевые возможности программного комплекса, перечислены предусмотренные в нем типы антенно-фидерных устройств, продемонстрирована обширность библиотеки импульсных сигналов, насчитывающая порядка ста комбинаций, описана логика функционирования модулей, при этом все основные этапы работы в программе проиллюстрированы рисунками. Сделан вывод о том, какую ценность представляет собой разработанный программный комплекс в решении поставленной задачи.

**Ключевые слова:** *корабельное радиоэлектронное средство, электромагнитная стойкость, мощное импульсное электромагнитное излучение, специализированный исследовательский программный комплекс, радиоэлектронная защита*

Проблема преднамеренных силовых воздействий на радиоэлектронные средства в последние годы приобрела большое значение в связи с развитием техники генерации, усиления и излучения мощных электромагнитных импульсов [1]. При разработке радиоэлектронных средств требования к ним по отношению к внешним электромагнитным возмущениям ужесточаются. Это влечет за собой повышение трудоемкости процесса разработки и требований к жёсткости испытаний, а, следовательно, увеличение временных, трудовых и материальных затрат [2, 3].

Сократить эти издержки становится возможным при помощи инструмента информационной поддержки принятия решений по снижению уровня взаимных радиопомех — специализированного исследовательского программного комплекса (СИПК), обеспечивающего проведение расчётно-оценочной экспертизы электромагнитной стойкости радиоэлектронных средств [4]. Применение СИПК на ранних этапах проектирования радиоэлектронных средств позволяет обосновать организационно-технические, конструктивно-технологические и структурно-схемотехнические решения, направленные на достижение заданного уровня радиоэлектронной защиты, а также существенно улучшить разработку программы и методик лабораторных, полигонных и натурных испытаний на этапе контрольно-инструментальной экспертизы радиоэлектронной защиты радиоэлектронных устройств к электромагнитным воздействиям и интерпретации протоколов таких испытаний.

Программный комплекс базируется на технологии расчётно-оценочной экспертизы стойкости радиотехнических систем, представляющей собой поэтапный анализ девяти различных уровней (контуров) рассматриваемого процесса воздействия мощного электромагнитного фактора [5]:

1. Сигнальный контур — анализ во временной области электромагнитного возмущения (мгновенной мощности), выдаваемого источником электромагнитного воздействия, с оценкой его параметров (форма, длительность, частота следования, длительность фронта, длительность среза, пиковое значение, время воздействия), анализ в частотной области электромагнитного возмущения, выдаваемого источником электромагнитного воздействия, с применением прямого быстрого преобразования Фурье для получения амплитудно-частотной (АЧХ) и фазо-частотной (ФЧХ) зависимости спектральной плотности мощности сигнала.

2. Фидерный контур источника — анализ параметров фидерного устройства (в том числе составного) источника электромагнитного воздействия с оценкой его АЧХ и ФЧХ коэффициента передачи и преобразования транслируемого электромагнитного возмущения.

3. Антенный контур источника — анализ параметров антенного устройства источника электромагнитного воздействия с оценкой его АЧХ и ФЧХ коэффициента передачи и преобразования излучаемого электромагнитного возмущения.

4. Траекторный контур — анализ параметров трассы распространения электромагнитного возмущения с оценкой её АЧХ и ФЧХ коэффициента передачи и преобразования излучаемого электромагнитного возмущения.

5. Антенный контур рецептора — анализ параметров антенного устройства рецептора электромагнитного воздействия с оценкой его АЧХ и ФЧХ коэффициента передачи и преобразования наводимого электромагнитного возмущения.

6. Фидерный контур рецептора — анализ параметров фидерного устройства (в том числе составного) рецептора электромагнитного воздействия с оценкой его АЧХ и ФЧХ коэффициента передачи и преобразования транслируемого электромагнитного возмущения.

7. Защитный контур — анализ параметров схемотехнических защитных устройств от мощных электромагнитных воздействий с оценкой его АЧХ, ФЧХ и переходной характеристики коэффициента передачи и преобразования транслируемого электромагнитного возмущения.

8. Компонентный контур — анализ параметров входных цепей и компонентов рецептора с оценкой их предельно-допустимых уровней (ПДУ) стойкости к мощным электромагнитным воздействиям (анализ во временной области электромагнитного возмущения, дошедшего до входных цепей и компонентов рецептора, с применением обратного быстрого преобразования Фурье (БПФ)).

При помощи численно-аналитического методического обеспечения, разработанного для каждого описанного уровня анализа рассматриваемого процесса воздействия мощного электромагнитного фактора, становится возможным проводить оценку применительно к морским радиотехническим системам различного назначения, функционирующим в различных диапазонах радиочастотного спектра.

Структуру вышеописанной модели наглядно иллюстрирует главная форма программы, показанная на рис. 1.

Рассмотрим работу данного программного обеспечения.

В программе предусмотрено два режима: ручной и графический.

Ручной режим (рис. 1) представляет собой последовательную работу с каждым из контуров электромагнитного взаимодействия. В каждом контуре пользователь задает необходимые параметры, и программа строит энергетико-временную, амплитудно-частотную и фазо-частотную зависимость сигнала, прошедшего данный контур. После чего в модуле компонентного контура рецептора пользователь получает заключение о характере производимого электромагнитного воздействия.

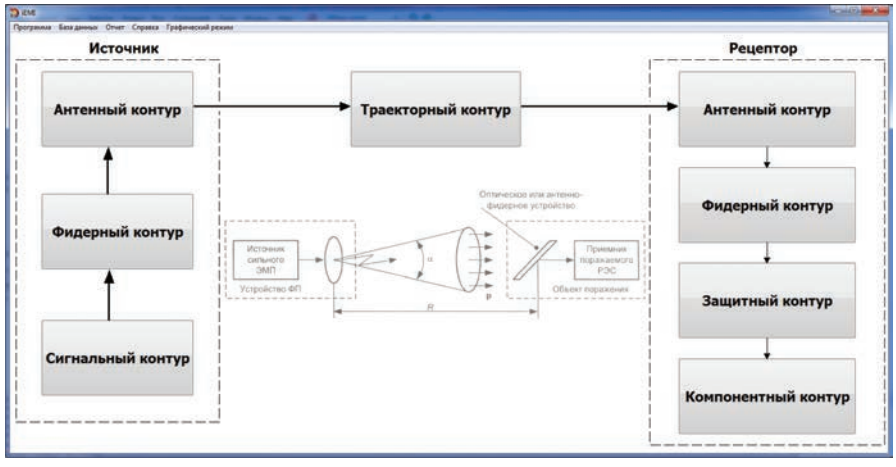



**Рис. 1.** Главная форма программы, ручной режим

В модуле сигнального контура источника имеется библиотека различных видов одиночных и периодических импульсных сигналов (рис. 2).

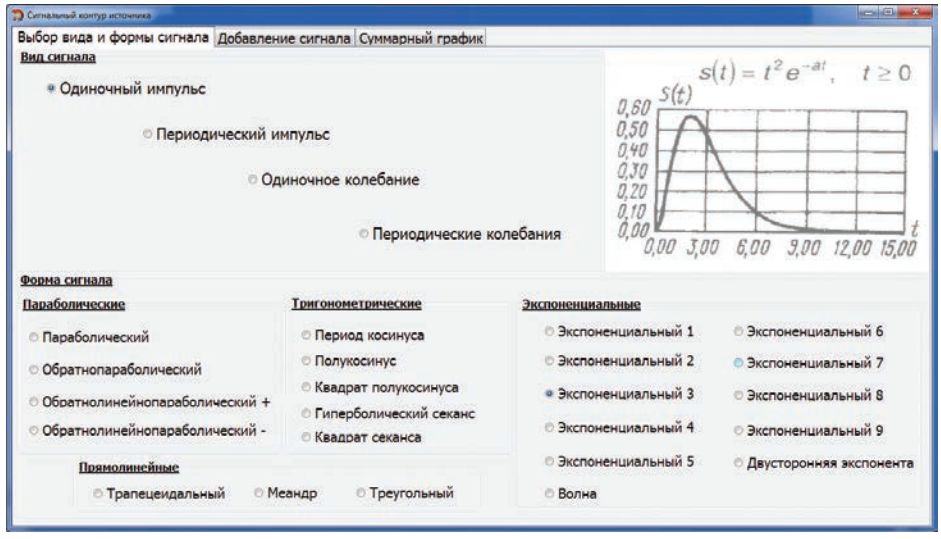



**Рис. 2.** Сигнальный контур источника. Выбор вида и формы сигнала

Суммарный излучаемый источником сигнал может быть составлен из множества парциальных сигналов различного типа, для которых можно рассчитать такие параметры как длительность фронта, среза, длительность импульса, энергия сигнала (рис. 3).

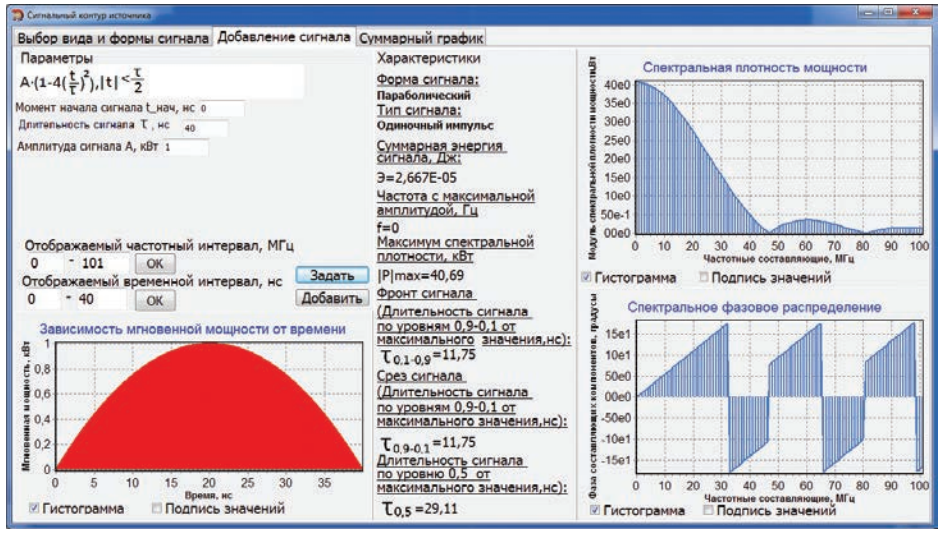



**Рис. 3.** Сигнальный контур источника. Добавление сигнала

При работе в фидерном контуре источника необходимо задать состав фидерного устройства (волновод круглый или прямоугольный, коаксиальный кабель) и его параметры либо загрузить передаточную характеристику устройства из txt-файла (аналогичная опция предусмотрена и для всех последующих контуров, что делает возможным импортирование в программу данных, полученных при работе в САПРе).

В антенном контуре источника существует возможность выбора одного из следующих видов антенных устройств: прямоугольная рупорная антенна, коническая рупорная антенна, H- и E-секториальные рупорные антенны, спиральная цилиндрическая и коническая антенны или зеркальная параболическая антенна.

Траекторный контур учитывает такие параметры как: высота расположения антенны источника, высота расположения антенны рецептора, расстояние между источником и рецептором, интенсивность дождя, видимость в тумане, скорость ветра, относительная влажность, температура воздуха.

В антенном контуре рецептора помимо устройств, предусмотренных в антенном контуре источника, для выбора доступны: антенна типа наклонный луч, штыревая антенна, вибраторная антенна, полосковая антенна и антенная решётка.

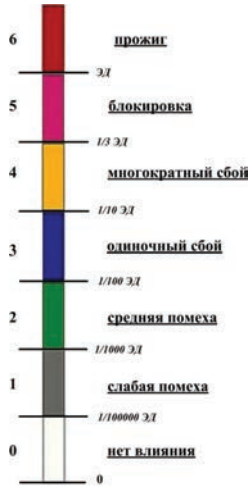



**Рис. 4.** Шкала оценки электромагнитного воздействия. ЭД — энергия деградации

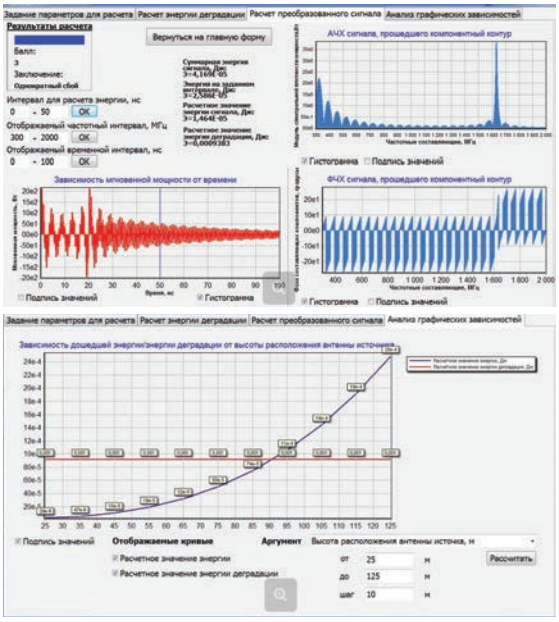


**Рис. 5.** Результаты расчета в ручном режиме

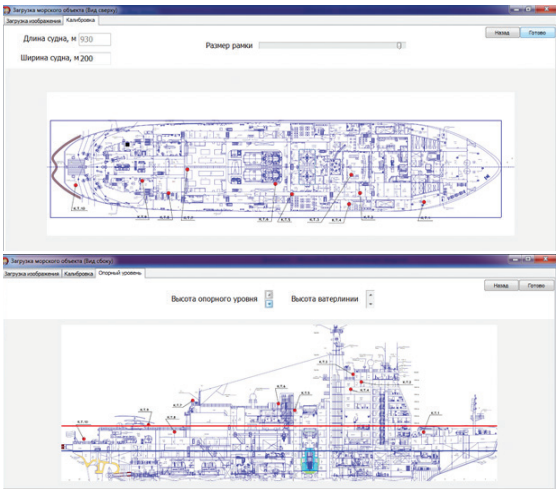


**Рис. 6.** Загрузка морского объекта. Калибровка и установка высоты ватерлинии и опорного уровня

В фидерном контуре рецептора помимо устройств, предусмотренных в фидерном контуре источника, для выбора доступны: круглая и квадратная высокочастотная шахта, полосковая линия, микрополосковая линия, двухпроводная линия.

При работе в защитном контуре рецептора существует возможность выбора из следующих защитных устройств: полосовой фильтр, фильтр низких частот, фильтр высоких частот.

В компонентном контуре необходимо ввести такие параметры элементной базы рецептора как: плотность, удельная теплоемкость, эффективная теплопроводность полупроводникового материала и прочие.

На основании всех введенных данных рассчитывается электромагнитная энергия дошедшего сигнала и энергия деградации входного полупроводникового устройства. В зависимости от соотношения этих величин программа выдает заключение о степени возможного ущерба РЭС с присвоением балла риска (рис. 4). Также существует возможность графического анализа дошедшей электромагнитной энергии сигнала и энергии деградации полупроводникового устройства от эксплуатационных факторов: высота расположения антенны источника, расстояние между источником и рецептором, амплитуда мощности генератора источника (рис 5).

Таким образом ручной режим позволяет произвести подробный расчет для одной пары источник-рецептор.

Графический режим позволяет провести расчет для множества антенн источников и рецепторов с учетом их трехмерного расположения на поле с морским объектом и сформировать сводную матрицу результатов расчетов с возможностью переключения в ручной режим для конкретной пары источник-рецептор.

Пользователь загружает изображение морского объекта в двух проекциях (вид сбоку и сверху), задает его размеры, производит калибровку, устанавливает высоту ватерлинии и опорного уровня (рис. 6).

Затем открывается форма для задания климатических условий, при которых происходит данное взаимодействие морского объекта с ракетами. После чего загруженный морской объект отображается на поле (рис. 7). Теперь пользователь может расположить на поле все необходимые ему антенны. Предусмотрена функция масштабирования поля с объектом как в меньшую, так и в большую сторону.

При установке на морском объекте рецептора, после того, как пользователь должным образом расположил антенну в обеих проекциях, последовательно открываются для заполнения модули антенного, фидерного, защитного и компонентного контура рецептора. Аналогично после установки на поле ракеты для неё запрашиваются данные по сигнальному, фидерному и антенному контуру источника.

Для всех установленных антенн формируется сводная матрица влияний (рис. 7). В столбцах расположены номера источников, в строках — номера рецепторов, на пересечениях — баллы по шкале оценки электромагнитного воздействия (рис. 4). Таким образом, сразу возможно оценить, какие из ракет наиболее опасны и какие из антенн наиболее уязвимы. Для более детального исследования пользователь может перейти в ручной режим для любой интересующей его пары источник-рецептор.

По результатам расчетов формируется база данных расчетных характеристик электромагнитной стойкости судовых РЭС различных диапазонов (рис. 8).

Текущий проект исследований можно сохранить или же открыть ранее созданный проект. Также существует опция генерации отчета в файл программное обеспечение MS Word.

Таким образом, разработанное программное обеспечение, являясь оперативным и удобным инструментом информационной поддержки

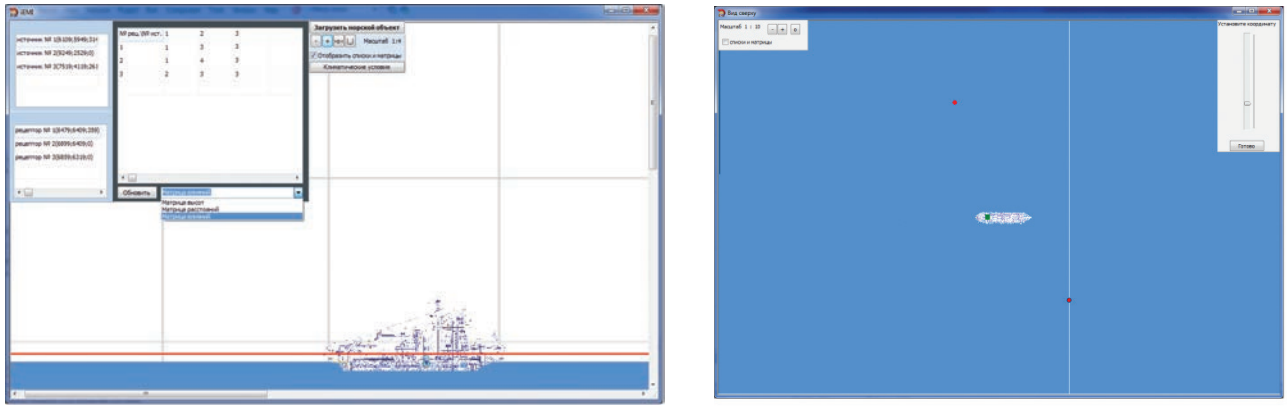


**Рис. 7.** Поле с морским объектом

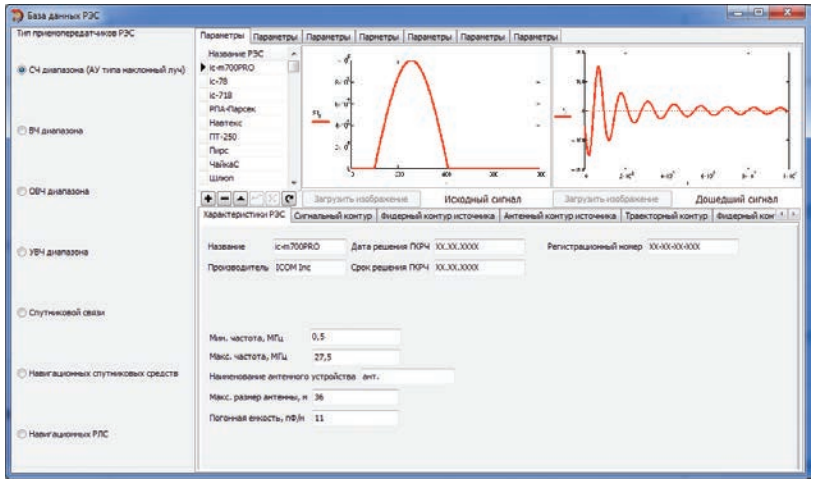


**Рис. 8.** Модуль базы данных

в вопросах снижения уровня взаимных радиопомех, позволяет сократить временные, трудовые и финансовые затраты при проектировании, проведении испытаний и приёмки радиоэлектронных средств по параметрам радиоэлектронной защиты.

Преимуществом предлагаемого подхода к расчётной оценке стойкости (РОСт) радиоэлектронных средств к мощным преднамеренным электромагнитным воздействиям является возможность анализа влияния каждого контура на прохождение рассматриваемого электромагнитного процесса и оценка их вклада в амплитудно-фазо-частотное преобразование структуры исследуемого электромагнитного возмущения. Преимуществом предлагаемого подхода к получению базы данных расчётных ПДУ относительно излучаемых мощных электромагнитных воздействий (МЭМВ) для исследуемых радиоэлектронных систем является возможность получения ряда таких оценок при вариации многочисленных видов и сочетаний исходных данных, относящихся как к МЭМВ (длительность фронта, пиковое значение, частота следования), так и к исследуемой радиоэлектронной системе (параметры фидерного тракта, характеристики антенного устройства).

**Список литературы**

1. Электромагнитный терроризм на рубеже тысячелетий / Под ред. Газизова Т. Р. Томск, Томский государственный университет, 2002. 204 с.

2. *Балюк Н. В., Кечиев Л. Н., Степанов П. В.* Мощный электромагнитный импульс: воздействие на электронные средства и методы защиты. М.: Группа ИДТ, 2007. 478 с.

3. *Бурутин А. Г., Балюк Н. В., Кечиев Л. Н.* Электромагнитные эффекты среды и функциональная безопасность радиоэлектронных систем вооружения // Технологии электромагнитной совместимости. 2010. № 1 (32). С. 3–27.

4. Свидетельство о государственной регистрации программы для ЭВМ № 2015616004. Расчетная оценка электромагнитной стойкости радиоэлектронных средств к воздействию мощных сверхкоротких импульсных электромагнитных излучений / Биктеева Анастасия Максимовна, Лазарев Дмитрий Владимирович; рег. от 28.05.2015, РОСПАТЕНТ.

5. *Лазарев Д. В.* Расчётный анализ стойкости средств радиолокации, навигации и связи к воздействию сверхширокополосных электромагнитных полей высокой интенсивности // XXI Международная научно-техническая конференция «Радиолокация, навигация, связь»: Сборник докладов. Воронеж: НПФ «САКВОЕЕ», 2015. С. 1402–1410.

## FEATURES SPECIALIZED SOFTWARE FOR CALCULATION AND ASSESSMENT EXAMINATION ELECTROMAGNETIC IMMUNITY SHIP REM

**Bikteeva Anastasiya Maksimovna**,
Moscow, Russia, nbikteeva@gmail.com

**Abstract**
The question of the possibility of solving the problem of the protection of ship radioelectronic means by intentional electromagnetic influences. As a tool to solve this problem, we propose the use of the research developed by the author of the specialized software based on settlement and valuation expertise electromagnetic immunity shipboard electronic systems to deliberate power electromagnetic effects as a tool for information support of decision-making in a given level of electronic protection. The concept underlying the present software means that, depending on the combination of factors electromagnetic interference may lead to information, functional or physical damage to electronic systems, and considers the interaction of the source of electromagnetic radiation and the device-receptor as a sequence of eight different levels of electromagnetic interference: the signal, feeder and antenna circuit source, trajectory loop, antenna, feeder, circuit protection, and the component of the receptor, each of which developed the calculated numerically-analytical methodical support. The calculations assumed exposure assessment electromagnetic defeat of seven-point scale, where 0 — no influence, 1 — a weak disturbance, 2 — average hindrance, 3 — failure of a single, 4 — multiple crashes, 5 — lock, 6 — burning. Considered in detail the progress made in the software package in two modes: graphical, takes into account the two-dimensional arrangement of a plurality of antenna sources and receptors and allows to generate a summary table of the results of calculations and manual allows for more detailed study for a specific pair of source-receptor. Are considered key features of software are listed therein prescribed types of antenna-feeder devices, demonstrate extensive library of pulsed signals, there are about a hundred combinations, described the logic of the functioning of the modules, all the main stages of the work program are illustrated in the drawings. The conclusion is, what value is the software package developed in the task.
**Keywords:** ship radio-electronic mean, electromagnetic immunity, powerful pulsed electromagnetic radiation, specialized research software package, radioelectronic protection

**References**
1. Gazizov N. R. (Ed.). *Elektromagnitnyi terrorizm na rubege tiysyacheletiy* [Electromagnetic terrorism of millennium]. Tomsk, Tomsk State University, 2002. 204 p. (In Russian)
2. Baluk N. V., Kechiev L. N., Stepanov P. V. *Moschnyi elektromagnitnyi impul's: vozdeystvie na elektronnyie sredstva I metodyi zaschityi* [The powerful EMP: effects on electronic means and methods of protection]. Moscow, Group of IDT, 2007. 478 p. (In Russian)
3. Burutin A.G, Baluk N. V., Kechiev L. N. Electromagnetic Environment Effects and functional safety of electronic weapons systems. *Technology EMC*. 2010. No. 1 (32). Pp. 3–27. (In Russian).
4. Certificate of state registration of the computer program № 2015616004. The estimated electromagnetic resistance of electronic means of ultrashort pulse to powerful electromagnetic radiation / Bikteeva Anastasia Maximovna, Lazarev Dmitry Vladimirovich; Reg. on 05.28.2015, ROSPATENT. (In Russian)
5. Lazarev D. V. Estimated immunity analysis of radar, navigation and communication systems to the impact of ultra-wideband electromagnetic fields of high intensity. XXI International Scientific-Technical Conference "Radiolocation, navigation, communication": Collection of reports. Voronezh: NPF "SAKVOEE", 2015. Pp. 1402–1410. (In Russian)

**Information about author:**
Bikteeva A. M., software engineer of 3 level, Central Research Institute “Kurs”.

# МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДВИЖЕНИЯ ГИПЕРЗВУКОВОГО ЛЕТАТЕЛЬНОГО АППАРАТА

**Пророк Валерий Ярославович,**
*д.т.н., профессор, профессор кафедры программно-алгоритмического обеспечения ракетно-космической обороны Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, val_prorok@mail.ru*

**Шаймухаметов Шамиль Ильдусович,**
*адъюнкт кафедры программно-алгоритмического обеспечения ракетно-космической обороны Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, 28_172@mail.ru*

**Аннотация**
В работе рассмотрены наиболее перспективные программы развития гиперзвуковых летательных аппаратов, их тактико-технические характеристики, проанализированы возможности и особенности движения, которыми обладают гиперзвуковые летательные аппараты, перечислены их основные преимущества, отражены наиболее вероятные способы запуска, приведена математическая модель движения гиперзвукового летательного аппарата в виде системы дифференциальных уравнений.

**Ключевые слова:** *гиперзвуковые летательные аппараты; крылатые ракеты; математическая модель движения.*

В настоящее время практически все промышленно развитые страны в стремлении обеспечить существенные преимущества в воздушно-космической сфере ведут активные исследования в области разработки перспективных гиперзвуковых технологий для создания нового поколения летательных аппаратов. Если первые проекты создания гиперзвуковых летательных аппаратов (ГЗЛА) были не подкреплены ни достаточной теорией, ни экспериментальными результатами, то уже к концу первого десятилетия нового столетия успешно прошли испытания и в основном сформировались класс и подклассы ГЗЛА. Определилась наиболее вероятная этапность создания и постановки новых типов летательных аппаратов на вооружение.

Наибольший объем опытно-конструкторских работ по созданию гиперзвуковых летательных аппаратов проводится в США. Основной концепцией, связанной с использованием ГЗЛА в качестве ударных средств, стала концепция Быстрого Глобального Удара (Prompt Global Strike — PGS). Генеральной задачей реализации концепции PGS является желание «иметь возможность в течение 60 минут нанести удар практически по любой точке на поверхности Земли».

Военно-промышленным комплексом совместно с научно-исследовательскими центрами США реализуется одобренная американским правительством широкомасштабная авиационно-космическая программа «Национальная авиационно-космическая инициатива» (NAI, National Aerospace Initiative), инициированная и руководимая управлением перспективных исследований Министерства обороны DARPA (Defence Advanced Research Projects Agency).

В рамках программы NAI осуществляется поэтапное освоение областей летных режимов ГЗЛА [1], которые, в отличие от других типов целей имеют ряд только им присущих особенностей, существенно затрудняющих решение задач по их обнаружению, сопровождению, опознаванию и поражению, возложенных на средства системы ПВО (ВКО) государства, против которого они будут применяться (рис. 1).

Первая — возможность использования ранее не освоенного (промежуточного) средствами воздушно-космического нападения диапазона высот от 30 до 120 км от земной поверхности.

Вторая — способность ГЗЛА осуществлять полет на ранее не достижимых для СВКН скоростях (от 5 до 30 М) как в атмосфере, так и за ее пределами — в околоземном космическом пространстве.

Третья — высокая вероятность боевого применения ГЗЛА на трансконтинентальных дальностях и последовательного перехода из воздушного пространства в космическое и обратно.

Четвертая — использование смешанных труднопрогнозируемых траекторий полета к объекту поражения (аэродинамическая — на начальном этапе полета, эллиптическая — при полете в околоземном космическом пространстве, баллистическая — на конечном этапе полета во время атаки объекта поражения (рис. 2)).

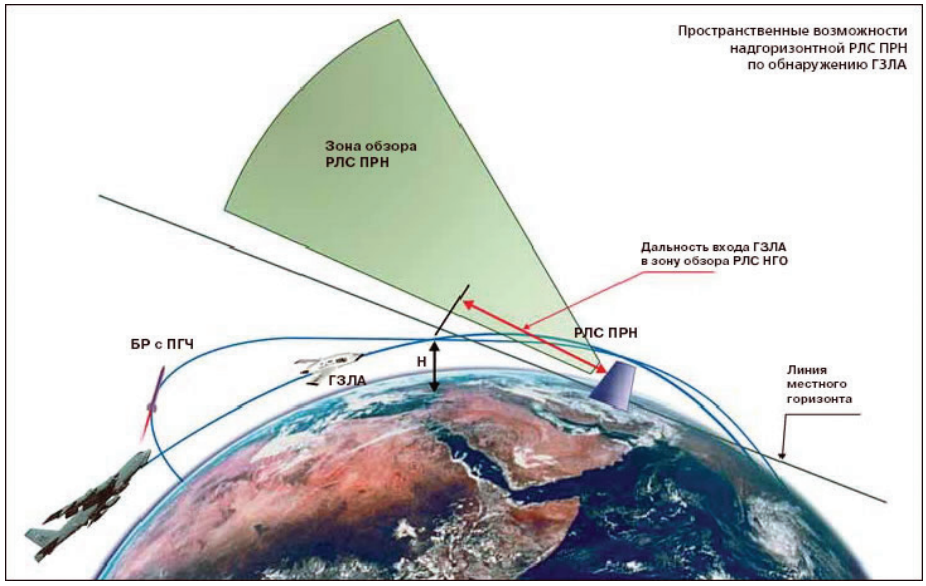



**Рис. 1.** Пространственные возможности РЛС по обнаружению ГЗЛА

Пятая — сочетание в одном ГЗЛА боевых свойств как аэродинамических СВН (способность совершать полет и маневрировать в атмосфере), так и космического аппарата (возможность нахождения на орбите и совершения маневра в ближнем космосе) [2].

Необходимо отметить, что в рамках концепции быстрого глобального удара и программы NAI МО США особое значение придает двум наиболее перспективным проектам: SED-WR (Scramjet Engine Demonstrator — Wave Rider) по созданию гиперзвуковой крылатой ракеты (ГЗКР) X-51A и FALCON (Force Application and Launch from CONtinental United States) по разработке серии ГЗЛА HTV (Hypersonic Technology Vehicle) и HCV (Hypersonic Common Vehicle) [3].

По мнению специалистов, расчетная дальность полета ГЗКР X-51A может составлять 1100 км, максимальная скорость полета 7–8 М, диапазон высот 10–30 км.

Военно-политическое руководство США рассматривает ГЗКР, прежде всего, в качестве высокоточных средств, с помощью которых можно оперативно уничтожать различные цели противника. Предполагается, что нанесение ударов данным ракетами будет осуществляться как по одиночным, так и по групповым особо важным стационарным и мобильным объектам. При этом носителями ГЗКР могут быть различные морские носители и стратегические бомбардировщики, а в перспективе самолеты тактической авиации и ударные беспилотные летательные аппараты [1].

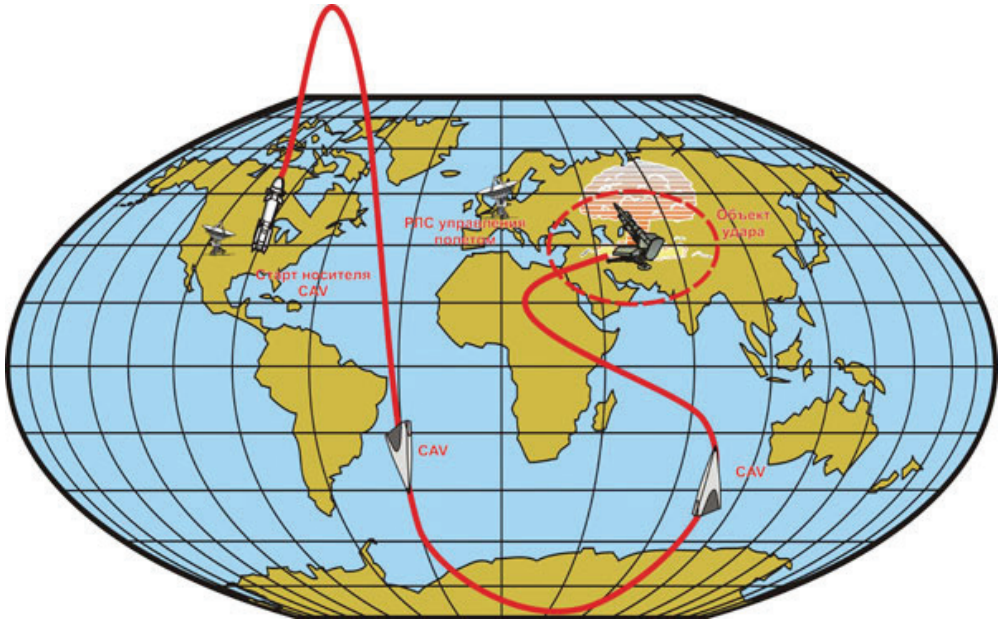



**Рис. 2.** Траектория возможного полета ГЗЛА

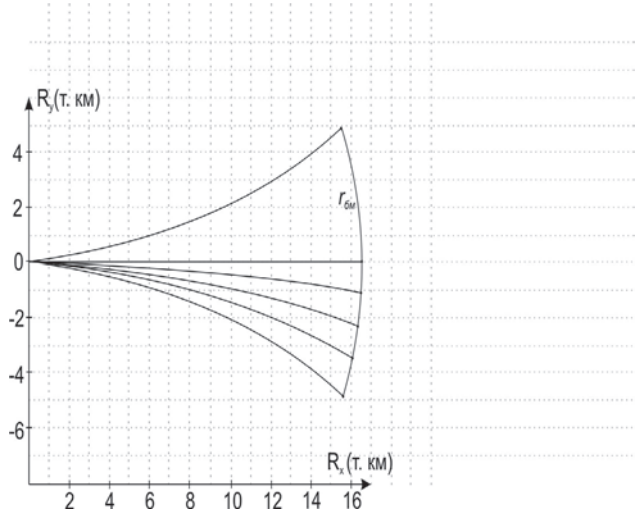



**Рис. 3.** Величина максимального бокового маневра ГЗЛА

В рамках проекта FALCON наибольший интерес представляют аппараты типа HTV, которые выводятся с помощью разгонных ступеней на высоту до 300 км, после чего происходит отделение разгонного блока и аппарат начинает снижение со скоростью порядка 20 М. Постепенно скорость снижается до 12 М, и на высоте 45 км начинается планирование, расчетная дальность которого составляет около 16500 км. Благодаря относительно высокому аэродинамическому качеству при такой дальности боковой маневр $r_{бм}$ составляет 5000 км (рис. 3). Большая скорость в момент удара вызывает мощный кинетический эффект.

ГЗЛА типа HTV имеет большие преимущества по сравнению с ГЗКР, наиболее важными из которых являются большая дальность полета и возможность осуществления старта с континентальной части США. ГЗЛА такого класса представляет собой маневренный гиперзвуковой планер, инерционный полет которого на межконтинентальную дальность обеспечивается за счет кинетической энергии, накопленной при работе ускорителей (разгонных ступеней). В качестве разгонных ступеней рассматриваются разнообразные варианты, в том числе различные ракетоносители и воздушно-космические системы. Полет аппарата осуществляется по траектории равновесного планирования либо по траектории динамического планирования с отражениями от плотных слоев атмосферы. Форма гиперзвукового планера обеспечивает ему достаточно большое значение аэродинамического качества во всем диапазоне гиперзвуковых скоростей полета. Это позволяет совершать длительный планирующий полет с разворотами на значительные расстояния в боковом направлении.

Учитывая рассмотренные выше тактико-технические характеристики и возможные особенности полета ГЗЛА система дифференциальных уравнений, описывающих их движение в траекторной системе координат, будет иметь вид [4]:

$$
\begin{cases}
\dot{V} = -\sigma_x \rho V^2 - g_r \sin\theta + g_z \sin\chi\cos\theta + \dfrac{P_x}{m} + \\
\qquad + R\Omega^2 \cos\varphi(\sin\theta\cos\varphi - \cos\theta\sin\varphi\sin\chi), \\
\dot{\theta} = \sigma_y \rho V \cos\gamma_a + \left(\dfrac{V}{R} - \dfrac{g_r}{V}\right)\cos\theta - \dfrac{g_z}{V}\sin\chi\sin\theta + \dfrac{P_y}{V_m} + \\
\qquad + 2\Omega\cos\varphi\cos\chi + \dfrac{R\Omega^2}{V}\cos\varphi(\cos\theta\cos\varphi + \sin\theta\sin\varphi\sin\chi), \\
\dot{\chi} = -\dfrac{\sigma_y \rho V}{\cos\theta}\sin\gamma_a - \dfrac{V\cos\theta}{R}\operatorname{tg}\varphi\cos\chi + g_z\dfrac{\cos\chi}{V\cos\theta} - \dfrac{P_z}{mV\cos\theta} - \\
\qquad - 2\Omega(\sin\varphi - \cos\varphi\sin\chi\operatorname{tg}\theta) - \dfrac{R\Omega^2}{V\cos\theta}\sin\varphi\cos\varphi\cos\chi, \\
\dot{R} = V\sin\theta, \\
\dot{\varphi} = \dfrac{V\cos\theta}{R}\sin\chi, \\
\dot{\lambda} = \dfrac{V\cos\theta}{R}\dfrac{\cos\chi}{\cos\varphi}, \\
\dot{m} = -\beta.
\end{cases}
\qquad (1)
$$

где $V$ — скорость,
$\theta$ — угол наклона траектории,
$\chi$ — угол пути,
$R$ — величина радиус-вектора центра масс ГЗЛА,
$\varphi$ — географическая широта,

$\lambda$ — географическая долгота,

$m$ — масса,

$\rho$ — плотность атмосферы,

$\Omega \approx 0,727 * 10^{-4} c^{-1}$ — угловая скорость вращения Земли вокруг своей оси.

Радиальная и трансверсальная составляющие вектора гравитационного ускорения $\vec{g}$, лежащего в меридиальной плоскости, с точностью до полиномов Лежандра второго порядка, определяются по формулам:

$$g_r = \frac{\gamma_3}{R^2}\left[1 + 0,00162\left(\frac{R_e}{R}\right)^2\left(1 - 3\sin^2\varphi\right)\right], \quad g_z = -0,00162\frac{\gamma_3 R_e^4}{R^4}\sin 2\varphi \tag{2}$$

где $\gamma_3 = 398600,4$ км$^3 / c^2$ — гравитационная постоянная Земли.

Проекции вектора силы тяги двигателей, жестко закрепленных и ориентированных вдоль продольной оси ГЗЛА, вычисляются по формулам:

$$\begin{aligned} P_x &= P\cos\alpha, \\ P_y &= P\sin\alpha\cos\gamma_a, \\ P_z &= P\sin\alpha\cos\gamma_a. \end{aligned} \tag{3}$$

где $P = P_{уд}\beta$ — сила тяги двигателей, $P_{уд}$ — удельная тяга.

Коэффициенты $\sigma_x$, $\sigma_y$ и аэродинамическое качество $K$ аппарата определяются по соотношениям:

$$\sigma_x = \frac{c_{xa}S}{2m}, \quad \sigma_y = \frac{c_{ya}S}{2m}, \quad K = \frac{c_{ya}}{c_{xa}} \tag{4}$$

где $c_{xa}$, $c_{ya}$ — коэффициенты аэродинамической силы лобового сопротивления и аэродинамической подъемной силы, $S$ — характерная площадь аппарата.

Число Маха рассчитывается как отношение воздушной скорости аппарата, которая при отсутствии ветра совпадает со скоростью относительно Земли, и скорости звука на данной высоте:

$$M = \frac{V}{a} \tag{5}$$

где скорость звука $a$ связана с температурой воздуха $T$ соотношением:

$$a = 20,0463\sqrt{T}$$

Высота $H$ над поверхностью Земли, имеющей форму эллипсоида вращения с указанными выше параметрами, вычисляется по формуле:

$$H = R - \frac{R_p}{\sqrt{1 - 0,0066934\cos^2\varphi}} \tag{6}$$

Составляющие вектора перегрузки в проекциях на связанную продольную и нормальную оси ГЗЛА определяются по соотношениям:

$$\begin{aligned} n_x &= \frac{P}{g_0 m} + \frac{S}{g_0 m}\frac{\rho V^2}{2}\left(c_{ya}\sin\alpha - c_{xa}\cos\alpha\right), \\ n_y &= \frac{S}{g_0 m}\frac{\rho V^2}{2}\left(c_{ya}\cos\alpha + c_{xa}\sin\alpha\right), \end{aligned} \tag{7}$$

где $g_0 \oplus 9,81 </A^2$ — гравитационное ускорение на поверхности Земли.

Скоростной напор $q$ и удельный тепловой поток $q_T$ в критической точке поверхности аппарата с радиусом кривизны $r_{кр}$ рассчитываются по формулам:

$$q = \frac{\rho V^2}{2}, \quad q_t = 0,95 \cdot 10^{-7}\sqrt{\frac{\rho}{r_{кр}}}V^{3,05}. \tag{8}$$

Таким образом, полученная математическая модель движения ГЗЛА, которая позволяет учитывать возможности полета по труднопрогрозируемым траекториям описывается с помощью представленных формул.

**Список литературы**

1. Лопин Г. А., Цурков М. Л., Оглоблин В. В. Угрожающая перспектива // Воздушно-космическая оборона. 2011. № 6.

2. Купцов И. М. Борьба с гиперзвуковыми летательными аппаратами: новая задача и требования к системе воздушно-космической обороны // Военная мысль. 2011. № 1. С. 10–17.

3. Кондратюк Е. Исследования, проводимые в США в области создания гиперзвуковых летательных аппаратов // Зарубежное военное обозрение. 2013. № 2. С. 63–69.

4. Лазарев Ю. Н. Управление траекториями аэрокосмических аппаратов. СНЦ РАН. 2007. С. 44–47.

## MATHEMATICAL MODEL OF MOVEMENT HYPERSONIC AIRCRAFT

**Prorok Valeriy Yaroslavovich,**
St. Petersburg, Russia, val-prorok@mail.ru.

**Shaymukhametov Shamil Ildusovich,**
St. Petersburg, Russia, 28_172@mail.ru

**Abstract**
In work the most perspective programs of development of hypersonic aircraft, their tactical technical characteristics are considered, possibilities and features of movement which hypersonic aircraft possess are analyzed, their main advantages are listed, the most probable ways of start are reflected, the mathematical model of movement of the hypersonic aircraft in the form of system of the differential equations is given.

**Keywords:** hypersonic aircraft; cruise missiles; mathematical model of movement.

**References:**

1. Lopin G. A., Tsurkov M. N., Ogloblin V. V. The menacing prospect. Air -space defense. 2011. No. 6. (In Russian)
2. Kuptsov I. M. Fighting hypersonic aircraft: a new challenge and requirements for the system of aerospace defense. Military Thought. 2011. No. 1. Pp. 10–17. (In Russian)
3. Kondratyuk E. Studies conducted in the United States in the field of hypersonic flight vehicles, postglacial. Foreign Military Review. 2013. No. 2. Pp. 63–69. (In Russian)
4. Lazarev Y. N. Path control of aerospace vehicles. SSC of RAS. 2007. Pp. 44–47. (In Russian)

**Information about authors:**
Prorok V.Y., Ph.D., professor, Military Space Academy;
Shaymukhametov S.I., postgraduate student, Military Space Academy.

# О НЕКОТОРЫХ ПРИНЦИПАХ УПРАВЛЕНИЯ СЕРВЕРНЫМ ОБОРУДОВАНИЕМ ЗАЩИЩЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Буренин Александр Николаевич,**
*д.т.н., доцент, профессор ВКА им. А.Ф. Можайского г. Санкт-Петербург,* konferencia_asu_vka@mail.ru

**Легков Константин Евгеньевич,**
*к.т.н., начальник кафедры ВКА им. А.Ф. Можайского г. Санкт-Петербург,* constl@mail.ru

**Первов Михаил Сергеевич,**
*старший офицер войсковой части 55297, г. Санкт-Петербург*

**Аннотация**
В статье показано, что функционирование современных инфокоммуникационных сетей специального назначения с высокими качественными показателями, может быть обеспечено только при решении комплекса задач управления их серверным оборудованием с учетом выполнения требований информационной безопасности.
Чрезвычайно сложная организация различных служб инфокоммуникационной сети специального назначения (информационных и телекоммуникационных) и механизмов их защиты приводят к тому, что возрастает число уязвимостей и потенциальных ошибок в использовании различных серверных средств, что обуславливают необходимость разработки оригинальных достаточно эффективных решений при организации текущего защищенного управления ими.
В статье рассматриваются некоторые принципы организации защищенного управления серверным оборудованием современных защищенных инфокоммуникационных сетей специального назначения, обеспечивающие выполнение требований по информационной безопасности, как при функционировании самих служб, так и при организации процессов технологического управления оборудованием.

**Ключевые слова:** *информационная безопасность; инфокоммуникационная сеть специального назначения; автоматизированная система управления; защищенное управление.*

В настоящее время в составе различных выделенных систем автоматизированного управления специального назначения создается так называемые инфокоммуникационные сети специального назначения (ИКС СН), являющиеся фактически информационным и телекоммуникационным ядром соответствующей системы управления и предоставляющей различным пользователям требуемые инфокоммуникационные услуги [1–5].

Функционирование таких ИКС СН с высокими качественными показателями в условиях достаточно жестких требований, предъявляемых к ним со стороны пользователей автоматизированных систем управления, возможно только при решении целого комплекса задач обеспечения информационной безопасности. При этом решающая роль в этом вопросе отводится программно-аппаратным комплексам средств автоматизации управления, которые должны осуществлять процессы управления оборудованием, учитывая возможности нарушителя или противника по проведению информационных воздействий на саму систему управления [6].

Возросшая сложность ИКС СН, входящих в состав систем организационного управления (абонентские сети, сети доступа, транспортная сеть, сети информационных и телекоммуникационных услуг), и требуемых механизмов их защиты, увеличение количества уязвимостей, потенциальных ошибок в использовании различных средств инфокоммуникаций, предоставления услуг и управления, а также возможностей потенциального нарушителя и противника по реализации различного рода кибератак, обуславливают необходимость разработки достаточно эффективных решений по обеспечению «защищенного режима» управления серверным оборудованием, которые, в свою очередь, существенно повышают защищенность самих серверов служб от возможных атакующих действий различных категорий нарушителей и противника.

Серверное оборудование инфокоммуникационных служб ИКС СН является достаточно сложным программно-аппаратным комплексом. Основные функции по его управлению сводятся к детальному мониторингу его состояния и вы-

работке (доведения) решений по изменению режимов его функционирования как элемента ИКС СН (класс задач управления уровня управления элементами сети в соответствии с концепцией TMN) [6].

При решении задач обеспечения информационной безопасности при управлении ИКС СН используются понятия моделей атак, нарушителя, объекта атак (инфокоммуникационная сеть, элементы сети) и т. д. [6].

Модель атак используется для описания возможных действий нарушителя или противника и формирования сценариев реализации этих действий. Она имеет вид иерархической структуры, состоящей из нескольких уровней.

Верхними уровнями являются комплексный и сценарный уровни. Комплексный уровень определяет множество высокоуровневых целей процесса анализа защищенности (анализ на нарушение основных аспектов информационной безопасности: целостности, конфиденциальности, доступности) и множество анализируемых (атакуемых) объектов. На комплексном уровне может быть обеспечено согласование нескольких сценариев, которые реализуются группой нарушителей или противником.

Сценарный уровень учитывает модель нарушителя (противника), определяет конкретный атакуемый объект выделенной ИКС СН (АРМ ДЛ ПУ, сервер службы и т. д.) и цель атаки (например, «определение типа операционной системы сервера», «реализация атаки отказа в обслуживании» и т. п.). Он содержит определенные этапы сценария, множество которых состоит из групп элементов: разведка, внедрение (первоначальный доступ к объекту атаки), повышение привилегий, реализация угрозы, сокрытие следов, создание потайных ходов. Элементы этого уровня, расположенные ниже, служат для детализации целей, достигаемых реализацией данного сценария. Нижний уровень в иерархии концептуальной модели атак описывает низкоуровневые атакующие действия нарушителя или противника.

Модель нарушителя (противника) тесно связана с моделью атак. Их взаимосвязь состоит в том, что в модели атак содержится максимально полное описание возможных способов компрометации объектов ИКС СН, а модель противника конкретизирует кто, какими средствами и с использованием каких знаний может реализовать данные угрозы и нанести ущерб тому или иному объекту. При этом сама модель должна учитывать основные параметры нарушителя или противника:

– первоначальное положение (внутренние и внешние нарушители);

– уровень знаний и умений, определяющий возможности противника, по реализации атакующих действий (задается перечнем известных противнику уязвимостей выделенной инфокоммуникационной сети, средств реализации атаки и т. п.);

– первичные знания об атакуемой выделенной инфокоммуникационной сети (например, в виде перечня АРМ ДЛ ПУ, коммутаторов, маршрутизаторов, серверов, пользователей и т. п.);

– используемый метод генерации сценария (используется ли оптимизация сценария для достижения заданной цели).

Для более подробного описания сценариев различных атак часто применяется модель формирования общего графа атак, которая служит для построения графовой модели, описывающей всевозможные варианты реализации атакующих действий противника с учетом его первоначального положения, уровня знаний и навыка, конфигурации ИКС СН, реализуемой в ней политики безопасности.

На основе графа атак производится анализ защищенности ИКС СН, определены «узкие» места сети, на основе чего могут быть выработаны рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности. В общем случае, при успешной реализации нарушителем или противником разведывательных действий, не происходит нарушения конфиденциальности, целостности и доступности информационных ресурсов ИКС СН. Однако, возможно нарушение конфиденциальности, например, в том случае, если политикой безопасности в сети установлено, что информация о топологии той или иной внутренней сети ИКС СН является закрытой. При успешном получении нарушителем или противником прав локального пользователя, возможности выполнения действий, направленных на нарушение конфиденциальности, целостности и доступности, или на получение прав администратора увеличиваются, так как, например, он может нарушить конфиденциальность, целостность и доступность некоторой совокупности объектов, имея только права пользователя.

При успешном получении прав администратора на определенном АРМе или сервере нарушитель или противник может полностью нарушить конфиденциальность, целостность, доступность всех объектов данного узла ИКС СН или даже ее фрагмента.

В направлении роста степени сложности все объекты ИКС СН обычно упорядочиваются следующим образом: элементы ИКС СН → атакующие действия → трассы атак → угрозы → общий граф атак.

После реализации каждого из сценариев, принадлежащих множеству сценариев разведки, производится проверка условий выполнения атакующих действий, использующих уязвимости программного и аппаратного обеспечения элементов выделенной инфокоммуникационной сети. При успешной реализации атакующих действий заданной группы, приводящих к получению нарушитель или противником прав локального пользователя или администратора на атакованном АРМе или сервере, осуществляется проверка необходимости перехода противника (нарушителя) на данный элемент сети. В случае реализации перехода, эта же последовательность действий повторяется для нового положения нарушитель или противника.

Модель ИКС СН служит для представления используемого в данной сети программного и аппаратного обеспечения, распознавания действий нарушителя или противника и определения реакции ИКС СН на реализуемые нарушителем или противником атакующие действия. Для спецификации аппаратного и программного обеспечения обычно используется

некоторый специализированный язык, использующий основные объектно-ориентированные технологии структурирования и концептуализации. При этом производится описание ИКС СН на уровне ее топологии и сетевых сервисов. Сетевая топология описывается классами физических элементов ИКС СН, связанных физическими линиями (цифровыми каналами, трактами), а сетевые сервисы — классами электронная почта, файловый обмен, диалоговый режим и т.д.

Другой моделью, используемой при решении задач обеспечения информационной безопасности ИКС СН, является модель оценки уровня защищенности, которая охватывает определенную систему различных метрик безопасности и правил, используемых для их расчета и оценки. При этом множество всех метрик безопасности строится на основе уже рассмотренного сформированного общего графа атак. Метрики безопасности обычно характеризуют защищенность как базовых, так и составных объектов графа атак и классифицируются по разделению объектов общего графа атак на базовые и составные, в соответствии с порядком вычислений, в соответствии с тем, используются ли метрики для определения общего уровня защищенности ИКС СН. Примерами метрик безопасности являются: критичность конкретного АРМа, сервера, коммутатора, маршрутизатора, размер ущерба при реализации угрозы, количество трасс атак на графе и т.д.

Традиционные методы защиты телекоммуникационных сетей в большей мере ориентированы на защиту от конкретных (известных или прогнозируемых) видов угроз и атак и реализуются в виде набора программных и аппаратных компонентов, функционирующих относительно независимо друг от друга. При этом существующие системы защиты обычно имеют централизованную структуру, характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, большим процентом ложных срабатываний при обнаружении вторжений, значительной деградацией трафика целевых информационных потоков из-за большого объема ресурсов, выделяемых на защиту и т.п. Процессы управления имеют существенные особенности.

Поэтому эффективные процедуры управления серверным оборудованием ИКС СН должны включать подзадачи контроля состояния различных функциональных его подсистем, сбора сведений о поступающих потоках писем, файловых запросов, требований на предоставление геоинформационных услуг и их обслуживании, о качестве обслуживания требований и пр. с включением в контур управления оператора автоматизированного рабочего места (АРМ) управления серверным оборудованием.

Менеджер АРМ содержит образ (модель) управляемого сервера, а также программную реализации процедур мониторинга состояния и оперативного управления каждым из них.

Замкнутые контуры управления серверным оборудованием защищенной ИКС СН характеризуются особенностями, связанными с обеспечением высоких требований по информационной безопасности процедур управления.

Состояния каждого элемента серверного оборудования отражаются в соответствующих положениях базы управляющей информации MIB. Для исключения влияния различных возмущений на реальное состояние серверного оборудования при обработке данных, считываемых с MIB, требуется применять как процедуры оценки случайных параметров из арсенала математической статистики, включая регрессионные модели, так и операторы текущей стохастической обработки данных мониторинга параметров, рассматриваемых как случайные процессы.

В современных серверах ИКС СН, диагностика состояния большинства модулей выполняется встроенными программно-аппаратными средствами с прогонкой специальных тестовых программ, что требует применения алгоритмов, в которых обоснованно выбраны характеристики процесса статистического сглаживания значений параметров оборудования, который осуществляется на основе их статистического анализа как случайных величин или случайных процессов, с выявлением функций и плотностей распределения (в том числе и многомерных). При этом основной задачей, которую необходимо решать при организации управления серверным оборудованием защищенной ИКС СН, является задача поддержания режима его функционирования с требуемыми показателями эффективности. Эта задача, как уже отмечалось, включает в себя подзадачу оперативного мониторинга состояния основных функциональных элементов серверного оборудования, которая должна решаться по схеме «менеджер-агент» с применением защищенных протоколов управления, среди которых в настоящее время известен и практически доведен до применения протокол SNMP v3 [6].

Однако, реальное применение этого протокола в практике управления натолкнулось на целый ряд проблем и трудностей, что привело к состоянию, когда основным протоколом, используемым в созданных и развертываемых ИКС СН, является протокол SNMP v2, характеризующийся весьма ограниченными и недостаточными показателями по информационной безопасности (без использования username и MD5 для аутентификации, шифрации и т.д.).

В целом при организации управления серверным оборудованием защищенной ИКС СН должен быть реализован целый комплекс средств обеспечения информационной безопасности (рис. 1), который должен включать:

- средства защиты информации управления от НСД;
- средства криптографической защиты информации управления;
- средства защиты информации управления от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН);
- средства обнаружения вторжений и атак.

Угрозы, используемые нарушителем или противником для НСД, определяются уровнем возможностей его доступа к оборудованию АСУ ИКС СН и ее программному обеспечению. Угрозами нарушения конфиденциальности информации при управлении серверным оборудованием ИКС СН являются:

- съем информации из открытых каналов управления;

– съем информации по техническим каналам ПЭМИН;
– несанкционированный обмен информацией между подсистемами АСУ;
– скрытая передача информации во внешние каналы.

Принципиальная возможность выполнения атак на систему управления ИКС СН в целом и, на подсистему технологического управления оборудованием (в т.ч. серверным) в частности, обусловлена следующими факторами:
– наличие информационных связей с внешней средой;
– использование недоверенной программно-аппаратной среды иностранного производства;
– применение готовых стандартных протоколов управления,
– хранение информационных ресурсов АСУ ИКС СН на материальных носителях информации, что может привести к преднамеренному или случайному их искажению;
– наличие опосредованного взаимодействия с внешней средой через систему электропитания и электромагнитные поля;
– участие человека (оператора или должностного лица) в принятии решений, эксплуатации и оперативном управлении серверным оборудованием ИКС СН.

Таким образом, общие требования к управлению серверным оборудованием ИКС СН (рис. 1) с точки зрения обеспечения информационной безопасности, сводятся:
– к применению сертифицированных программно-аппаратных средств;
– к применению криптографической защиты всей управляющей информации (абонентское и линейное в канале управления засекречивание);
– к организации контроля целостности информации, передаваемой по каналам управления;

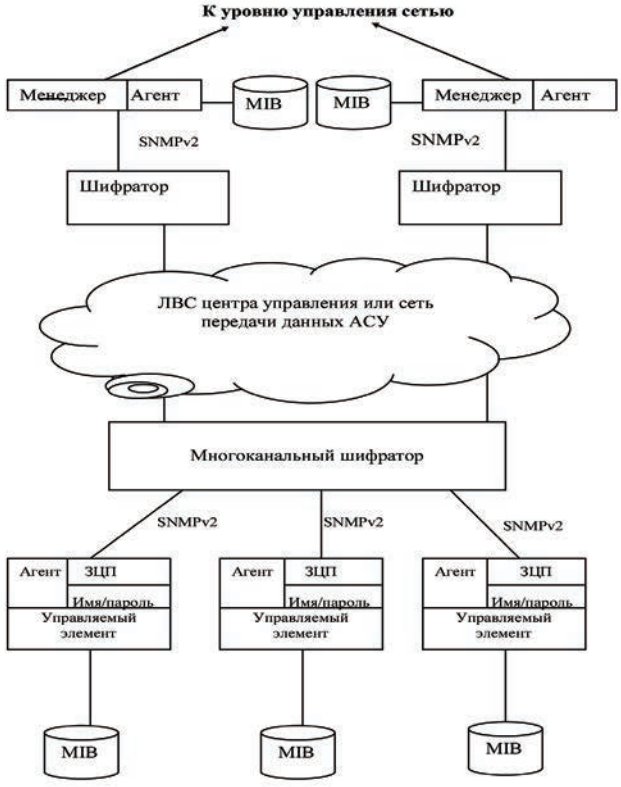



**Рис. 1.** Меры по обеспечению информационной безопасности при применении стандартных протоколов управления серверным оборудованием ИКС СН

– к широкому применению технологии электронной цифровой подписи (ЭЦП) при организации обмена управляющей информации;
– к применению алгоритмов исключающих или существенно снижающих вероятность нарушения работоспособности;
– к реализации на прикладном уровне протоколов взаимной аутентификации менеджеров и их агентов.

Кроме того, для исключения возможности несанкционированной модификации управляющей информации целесообразно применение специальных маскировочных методов манипуляции содержимым MIB, предполагающих периодическое изменение параметров и значений определенных элементов MIB по псевдослучайным маскам, имеющимся как у менеджеров, так и у агентов технологического управления серверным оборудованием (рис. 2).

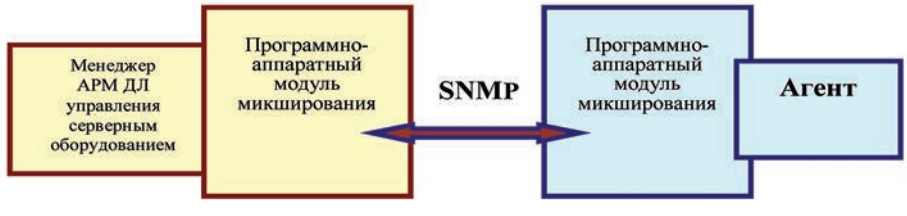



**Рис. 2.** Схема изменения элементов MIB при передаче их протоколом SNMP с помощью алгоритмов, реализованных в программно-аппаратном блоке микширования

**Список литературы**

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

2. *Буренин А.Н., Легков К.Е.* Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 3. С. 12–17.

3. *Буренин А.Н., Легков К.Е.* К вопросу математического описания потоков управляющей информации в процессе управления современной инфокоммуникационной сетью специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 5. С. 8–12.

4. *Буренин А.Н., Легков К.Е.* Особенности организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 2. С. 34–41.

5. *Буренин А.Н., Легков К.Е.* Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2011. Т. 3. № 2. С. 19–23.

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

## SOME PRINCIPLES OF SERVER HARDWARE CONTROL OF PROTECTED INFOCOMMUNICATION NETWORKS OF SPECIAL PURPOSE

**Burenin Andrey Nikolaevich,**
St. Petersburg, Russia, konferencia_asu_vka@mail.ru

**Legkov Konstantin Evgen'evich,**
St. Petersburg, Russia, constl@mail.ru

**Pervov Mihkail Sergeevich,**
St. Petersburg, Russia

**Abstract**
It is shown that the functioning of modern infocommunication networks of special purposes with high quality indicators, can only be achieved in solving complex control tasks of their server hardware, taking into account the implementation of information security requirements.
Extremely complex organization of different infocommunication network services of special purpose (information and telecommunication) and defense mechanisms lead to the fact that an increasing number of vulnerabilities and potential errors in the use of various server resources, which calls for the design of the original enough for effective solutions in the organization of the current secure control.
In this article some of the principles of the organization of management of the protected server hardware today protected info-communications networks for special purposes, ensuring the implementation of information security requirements, such as in the operation of the services themselves and the organization of technological processes control equipment are considered.
**Keywords:** information security; infocommunication network of special purpose; automated control system; protected control.

**References:**
1. Burenin A.N., Legkov K.E. Modern infocommumication and networks of special purpose. Basics of construction and control. Monograph. Moscow, Media Publisher. 2015. 348 p. (In Russian)
2. Burenin A.N., Legkov K.E. Features of the architecture, operation, monitoring and control of field components of modern infocommunication networks of special purpose. H&ESResearch. 2013. Vol. 5. No. 3. Pp. 12–17. (In Russian)
3. Burenin A.N., Legkov K.E. On the question of the mathematical description of control information flows in the control process of modern infocommunication network of special purpose. H&ESResearch. 2013. Vol. 5. No. 5. Pp. 8–12. (In Russian)
4. Burenin A.N., Legkov K.E. Features of the organization of control processes of infocommunication networks of special purpose. H&ESResearch. 2015. Vol. 7. No. 2. Pp. 34–41. (In Russian)
5. Burenin A.N., Legkov K.E. Monitoring process models while providing operational control operation of infocommunication networks of special purpose. H&ESResearch. 2011. Vol. 3. No. 2. Pp. 19–23. (In Russian)
6. Burenin A.N., Kurnosov V.I. Theoretical bases of control of modern telecommunications networks. Monograph. Moscow, Nauka. 2011. 464 p. (In Russian)

**Information about authors:**
Burenin A.N., Ph.D., associate professor, associate professor of the Department automated systems of control, Military Space Academy;
Legkov K.E., Ph.D., deputy head of the Department automated systems of control, Military Space Academy;
Pervov M.S., Senior officer of military unit 55297.

# О ПРИМЕНЕНИИ НЕЧЁТКИХ ПРОДУКЦИОННЫХ МОДЕЛЕЙ В ПОДСИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Клянчин Валерий Константинович,**
*директор Пензенского филиала ФГУП «НТЦ «Атлас», г. Пенза, Россия, atlas@sura.ru*

**Сашников Тимур Касимович,**
*заместитель директора Пензенского филиала ФГУП «НТЦ «Атлас», г. Пенза, Россия, atlas@sura.ru*

**Аннотация**
Информационные и телекоммуникационные ресурсы автоматизированных систем управления специального назначения в настоящее время подвергаются всё более многочисленным злонамеренным атакам, представляющих серьёзную угрозу обороноспособности государства и безопасности его граждан. В связи с этим при создании подсистем информационной безопасности критически важных технических систем одной из главных задач является обеспечение необходимого уровня качества защиты информационных ресурсов с учётом специфики условий функционирования, требований по противодействию постоянно совершенствующимся деструктивным попыткам воздействий нарушителей различного уровня подготовки и оснащённости, а также реализации возможностей по эффективному функционированию в динамически меняющихся условиях. Качественное совершенствование принципиально важных свойств подсистем информационной безопасности всё больше связывают с активным применением интеллектуальных средств обработки данных. Подобный инновационный подход предоставляет возможность применять при создании средств информационной безопасности новейшие технологии на основе извлечения и обработки знаний. Рассматриваемая концепция основывается на архитектуре, включающей в себя следующие структурные компоненты: экспертную подсистему, телекоммуникационную среду, подсистему информационной безопасности, операционную среду, базу нечётких продукционных правил, конвертор дискретных данных в правила. Источниками знаний о предметной области являться как практический опыт экспертов, так и информация мониторинга внешней среды и внутренних источников. Знания представляются в форме нечётких продукционных правил, которые могут быть обработаны совместно с входными данными с использованием аппарата нечёткого продукционного вывода. В качестве примера показаны конкретные механизмы реализации идеологических подходов с использованием искусственных нейронных сетей и нечёткой логики. Рассмотрены вопросы извлечения нечётких правил из дискретных данных на основе известных методов, один из которых представлен в статье. При использовании предлагаемых концепций построения системы обеспечения информационной безопасности представляется возможным создавать защищённые информационные системы, обладающие новыми возможностями в части предоставления эффективного интерфейса взаимодействия с экспертами, учёта опыта функционирования, адаптации к изменениям, эволюционного развития, в совокупности позволяющими обеспечить надёжную защиту АСУ специального назначения.

**Ключевые слова:** *автоматизированная система управления; информационная безопасность; экспертная система; база знаний; продукционные правила; нечёткий логический вывод; нечёткие множества; функция принадлежности; фаззификация; искусственная нейронная сеть.*

Возрастание уровня и интенсивности проявления угроз информационной безопасности (ИБ) для автоматизированных систем управления специального назначения (АСУ СН) является одной из актуальнейших и сложнейших проблем настоящего времени. Одним из инновационных направлений развития современных информационных технологий является разработка и применение принципиально новых подходов в сфере мониторинга защищённости и обеспечения информационной безопасности в сложных технических системах, включая АСУ СН и, в том числе, с использованием методов интеллектуального анализа данных и инженерии знаний. Это обусловлено заметным усложнением в последние годы задач защиты информационных ресурсов, а также наметившимся прогрессом в исследованиях и разработках по проблематике искусственного интеллекта.

Особенностями обеспечения информационной безопасности (ОБИ) для АСУ СН являются высокая динамика, скоротечность и сложность протекающих в них процессов, регулярное проявление событий со значительной степенью си-

туационной неопределённости, постоянное видоизменение и возникновение новых типов злонамеренных вторжений, значительная вероятность атак на информационные и телекоммуникационные ресурсы, высокая стоимость рисков при преодолении нарушителями защитных механизмов. Учитывая это, к средствам обеспечения информационной безопасности предъявляются самые высокие требования, в том числе к наличию свойств оперативной адаптации при функционировании в самых сложных условиях применения.

Недостатком современных средств обеспечения ИБ (СОИБ) АСУ СН является возможность противодействия только заранее известным угрозам. СОИБ, построенные на основе традиционных подходов, во многих случаях становятся неэффективными при отражении атак с новыми ранее неизвестными свойствами [1]. В связи с этим разработка перспективных СОИБ в последнее время всё более ориентируется на активное применение интеллектуальных средств, таких как: экспертные системы, системы нечеткой логики, искусственные нейронные сети, генетические алгоритмы, вероятностные вычисления, а также на их совместное гибридное использование. Подобный новый подход делает возможным реализацию в СОИБ принципиально новых свойств, таких как адаптируемость к изменениям, возможности по самоорганизации, способности к обучению и эволюционному развитию с унаследованием лучших полезных качеств.

При использовании потенциала этих интеллектуальных средств могут быть успешно решены задачи классификации и кластеризации угроз ИБ, мониторинга состояний и оценки степени защищённости АСУ СН, извлечения знаний из баз данных и информационных потоков, оценки рисков, моделирования и прогнозирования развития событий, ситуационного поведения в условиях неполной определённости [5]. Принципиально новым направлением в проектировании систем защиты информации является использование, наряду с методами обработки дискретных данных, дополнительных механизмов, обеспечивающих включение в контур систем защиты информации технических средств и процессов работы с новой категорией — структурированными знаниями.

Одним из архитектурных подходов в построении средств информационной защиты является включение в их состав экспертных систем, дающих возможность «интеллектуализировать» процессы управления на основе использования знаний и практического опыта компетентных специалистов. Понятие экспертной системы, функциями которой обычно является поддержка принятия решения субъектом управления (оператором или техническими средствами), осуществляющим контроль функционирования технической системы, предполагает организацию процессов получения, хранения и применения знаний из конкретной сферы жизнедеятельности. Естественно, что при этом принципиальным моментом является не тождественность природы таких категорий как данные и знания.

Исходными предпосылками создания перспективных эффективных СОИБ, является специфика этой предметной области, обладающей ярко выраженной слабой структурированностью и, одновременно, высокой степенью ситуационной неопределённости. С учётом этой специфики одним из способов удовлетворения современных требований информационной защиты является построение средств защиты на основе нейро-сетевых структур с элементами экспертной системы, использующей нечёткие продукционные модели [6].

Основой любой современной АСУ СН является входящая в её состав информационная система (ИС). Данная концептуальная модель ИС включает в себя обычно следующие основные структурные блоки, представляющие интерес в рассматриваемом контексте: экспертную подсистему, телекоммуникационную составляющую, подсистему информационной безопасности, операционную среду ИС, базу продукционных правил, конвертор дискретных данных в знания (рис. 1).

Экспертная подсистема в данном случае является источником представлений о предметной области защиты информации в среде конкретной информационной системы. Эти представления формируются опытными экспертами из области информационной безопасности и оформляются, как будет показано ниже, в виде нечётких правил [2] с использованием специального интерфейса и после соответствующего преобразования вводятся в базу нечётких продукционных правил.

Другим источником знаний является информационные сигналы, поступающие из внешней среды, а также от внутренних источников, сведения о которых записываются в базу данных операционной среды ИС. Связь базы знаний с базой данных осуществляется посредством конвертора, по сути выполняющего извлечение знаний из данных.

Одной из основных функций защиты является выработка оптимальной линии поведения, обеспечивающей эффективную защиту от угроз информационной безопасности. Это осуществляется на основе агрегированных знаний, представляющих собой совокупность экспертных оценок и новых знаний об изменениях в окружающей и внутренней среде, в том числе и актуальные знания об уязвимостях и угрозах информационной безопасности. На основе линии поведения могут быть организованы процессы обеспечения принятия решений для приведения в действие механизмы информационной защиты, а также запущены процессы адаптации, которые, соответственно, отражаются в базе знаний.

Следует отметить, что для обеспечения высокой надёжности и устойчивости функционирования подобной системы, имеющей признаки саморегулирования, необходимо наличие механизма обратной связи, заключающегося в регулярной оценке эффективности вносимых изменений в линию поведения, механизмы защиты и адаптации. Дополнительно в целях укрепления доверия к формируемым результатам требуется наличие функционала, обеспечивающего доступную для понимания аргументацию получаемых решений задач.

Авторы полагают, что на основе описанной концепции становится возможным реализовать достаточно обширный набор полезных с точки зрения защиты информации задач и качеств, таких как: распознавание угроз, динамический мониторинг внутренних состояний и внешних воздействий [7], возможность автоподстройки своих рабочих параметров

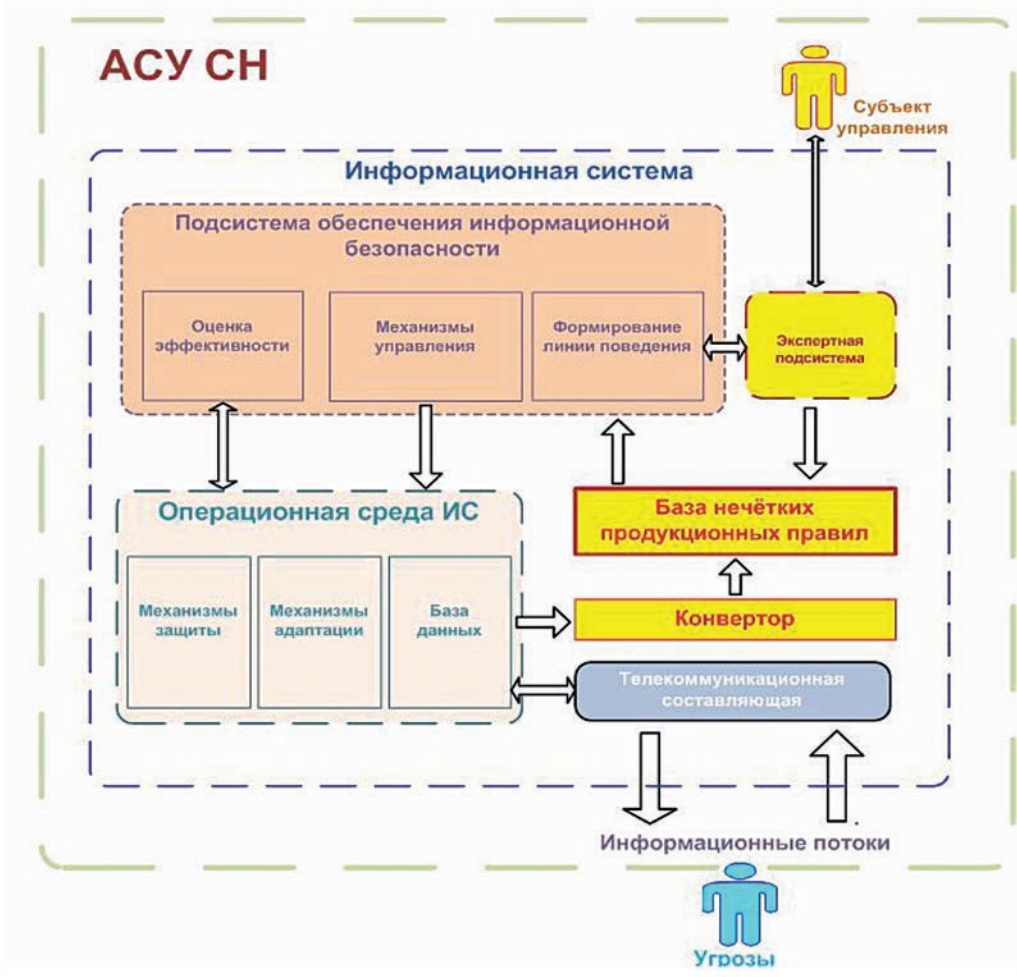



**Рис. 1.** Структура АСУ СН, с подсистемой обеспечения ИБ и экспертной подсистемой

под меняющиеся условия, способность прогнозирования изменений обстановки по безопасности, анализ рисков с возможностью приведения в действие механизмов по их максимальной компенсации, высокий начальный уровень знаний и способность автоматически пополнять знания, извлекая их из внешнего информационного потока или последовательности событий при функционировании в реальных условиях, возможность нахождения правильных решений в условиях неполной определённости.

Предлагаемый идеологический подход, базируется на категориях продукционных правил и ориентирован на использование теории нечётких множеств и аппарата нечёткой логики. Его суть состоит в том, что правила представляются в нечёткой интерпретации, на основе понятия базового правила вывода. Базовое правило вывода, называемое импликацией, имеет следующий вид:

если x это A, то y это B,

где A и B — это нечёткие множества, определяемые через функции принадлежности для переменных x и y соответственно. Левая часть правила «x это A» называется условием (предпосылкой), а правая часть «y это B» — следствием (заключением). В общем случае условие принимает многомерный вид:

если $x_1$ это $A_1$ и $x_2$ это $A_2$ и…и $x_N$ это $A_N$ то y это B.

Решение формируется в соответствии с классической схемой нечёткого вывода (рис. 2).

В качестве реализации механизма получения решения рассмотрим, нейро-нечёткую сетевую структуру на примере продукционной сети Ванга-Менделя (рис. 3). Следует заметить, что существует целый ряд признанных научным сообществом нейро-нечётких структур, позволяющих получать решения на основе использования продукционных моделей (Мандани, Цукамото, Ларсена, Такаги-Сугено, и др.). При разработке конкретных инженерных проектов реализации продукционных механизмов следует анализировать поставленную задачу на предмет оптимального выбора конкретной нейро-нечёткой структуры с учётом наличия имеющихся для этого аппаратно-программных ресурсов с гарантией полу-

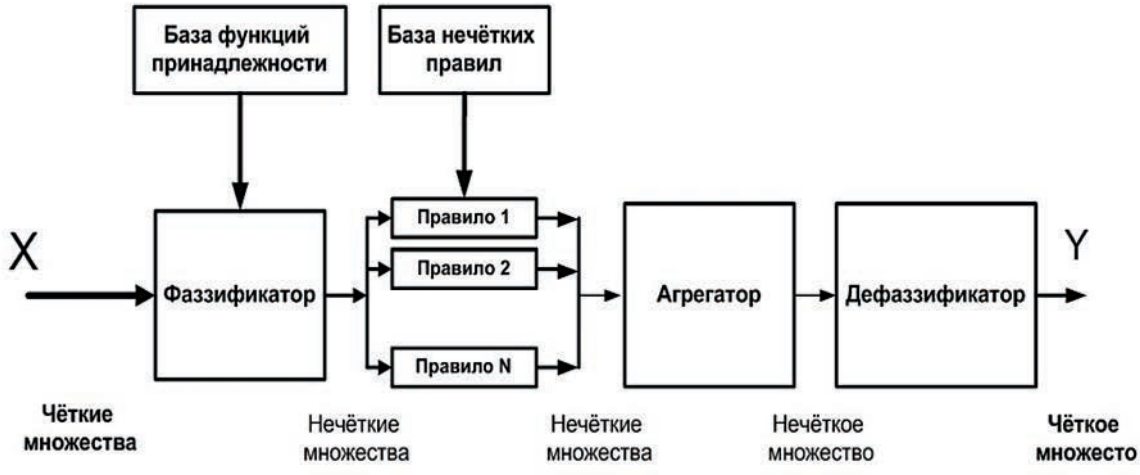



**Рис. 2.** Схема получения решения с использованием методов нечёткой логики

чения приемлемых временных характеристик, эффективности алгоритмов её обучения и ряд других аспектов. Самым эффективным средством при решении этих вопросов является моделирование, тем более, что в настоящее время в настольных моделирующих системах, например MATLAB, обычно включаются приложения, предоставляющих необходимые сервисы моделирования нейро-сетевых структур.

Сеть представлена четырьмя слоями, при этом:

– первый слой выполняет фаззификацию входных переменных в отношении функции принадлежности, задаваемой «гауссовским» распределением;

– второй — агрегирование значений отдельных переменных $x_j$ в условии $i$-го правила вывода;

– третий — агрегирование $M$ правил вывода (верхний нейрон) и генерацию нормализующего сигнала для четвёртого слоя (нижний нейрон);

– четвёртый слой, представленный единственным нейроном, осуществляет нормализацию, формируя выходной сигнал Y.

В данной структуре только первый и третий сетевые слои являются параметрическими с подбираемыми параметрами при обучении ИНС. В первом слое это параметры гауссовской функции фаззификации $c_j^{(i)}$, $b_j^{(i)}$, $\sigma_j^{(i)}$, а в третьем слое — веса, интерпретируемые как центр $c_i$ функции принадлежности экспертного заключения $i$-ого нечеткого правила вывода. Обучение сети может быть проведено с использованием алгоритмов на основе одного из известных методов, подробно рассмотренных в литературе [3,4]. Нетрудно догадаться, что материалом для обучения является база знаний, представленная в виде нечётких продукционных правил.

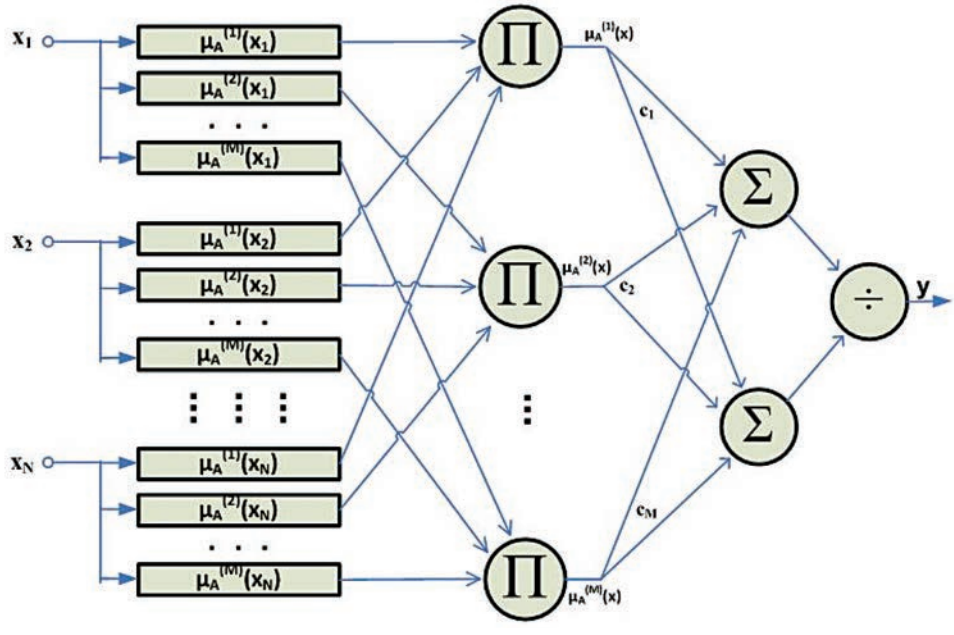



**Рис. 3.** Нейро-нечёткая сеть Ванга-Менделя

Преимуществом предлагаемого подхода на основе применения продукционной модели являются взаимная увязка:

а) достоинств экспертной системы, способной оперировать знаниями с возможностью видоизменять знания при развитии обстановки по безопасности (в данном случае речь идёт об автоматизированном способе с участием экспертов);

б) достоинств методов нечёткой логики в части представления экспертных правил в нечёткой форме, с одной стороны доступных для понимания человеком, с другой стороны поддающихся обработке вычислительными средствами;

в) достоинств ИНС, имеющих мощный механизм получения решения, дополняемый возможностью машинного обучения на продукционных правилах в нечёткой форме.

Одним из достоинств нечётких продукционных моделей является наличие возможности решения задачи автоматического извлечения продукционных правил из численных данных. Известно несколько способов решения подобной задачи, наиболее простым и наглядным из которых, по мнению авторов, является подход описанный в литературе [3], основная идея которого заключается в изначальном группировании данных по категориям входных данных с подгруппами, соответствующими отдельным входным численным переменным $x_1, x_2, \ldots x_N$, и выходным значением функции $Y$ (рис. 4). Далее определяется диапазон изменения величин в рассматриваемых подгруппах простым нахождением минимального и максимального значения и, соответственно, определением интервала изменения параметров. Интервал по каждому параметру разбивается на отдельные участки, на которых выбирается определённый вид функции принадлежности («гауссовский», треугольный, трапецеидальный и пр.). Затем выполняется формирование нечётких правил в предварительном, «огрубленном» виде на основе поочерёдного сопоставления значений параметров в подгруппах, описывающих переменные $x_1, x_2, \ldots x_N$, с представлением $Y$. Затем выполняется нормализация правил, устраняющая противоречивость отдельных пар термов правил и избыточность, возникающая из-за повторяемости термов. Последним шагом в алгоритме является собственно создание базы нечётких правил, представляющую собой базу знаний, фильтрацию правил в пересекающихся диапазонах с одинаковой посылкой (при этом выбирается правило, имеющее наибольшую степень истинности).

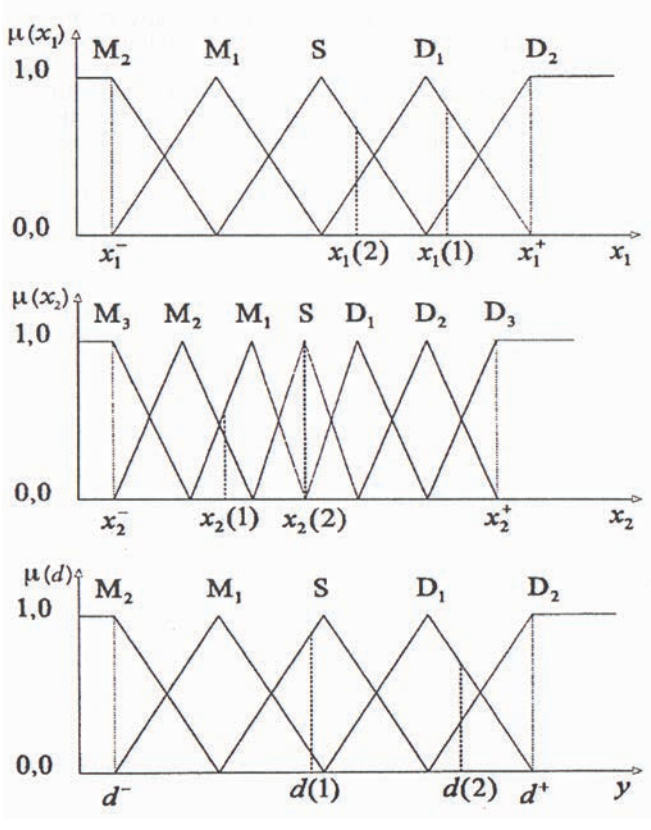



**Рис. 4.** Иллюстрация метода извлечения нечётких правил из данных

При использовании данного алгоритма извлечения знаний представляется возможным дополнять имеющуюся базу правилами, созданными на основе численных данных, полученных из среды окружения целевой системы. Этот интеллектуальный ресурс позволяет повысить эффективность экспертов, например, в части создания более полной базы знаний, охватив дополнительно случаи, которые по каким-либо причинам могли быть упущены экспертами, и, в том числе, ранее им не известные, включая случаи ситуаций, ранее считавшихся неопределёнными. На основании извлечённых и накопленных продукционных правил предоставляется возможность распознавать ту или иную ситуацию, предложить варианты решений по выбору действий в конкретной обстановке, что в целом будет способствовать принятия более качественных решений.

Таким образом, предлагаемые концептуальные подходы к построению средств защиты информации с использованием баз знаний с представлением их в виде продукционных правил позволяют создавать защищённые информационные системы, обладающие новыми возможностями в части предоставления интерфейса взаимодействия с экспертами, учёта опыта функционирования, адаптации к изменениям, эволюционного развития, в совокупности позволяющими обеспечить более эффективную защиту информационных систем.

**Список литературы**

1. *Бородакий Ю. В.* и др. Перспективные системы защиты информации должны быть интеллектуальными» // Защита информации, INSIDE. 2013. № 2. С. 48–51.

2. *Абрахам А.*, *Семченко П Н.* Основанные на правилах экспертные системы // Ученые заметки ТОГУ. 2014. Т. 5. № 4. С. 1249–1266.

3. *Рутковская Д.*, *Пилиньский М.*, *Рутковский Л.* Нейронные сети, генетические алгоритмы и нечёткие системы. М.: Горячая линия — Телеком. 2007. 452 с.

4. *Борисов В. В.*, *Круглов В. В.*, *Федулов А. С.* Нечёткие модели и сети. М.: Горячая линия — Телеком, 2012. 284 с.

5. *Сашников Т.К.* К вопросу применения методов интеллектуального анализа данных в технологиях обеспечения информационной безопасности мобильных комплексов связи // Труды XVIII Международной научно-технической конференции «Инноватика-2013». М.:, Энергоатомиздат, 2013. С.132–134.

6. *Сашников Т.К.* О прикладном значении «мягких вычислений» для решения задач обеспечения информационной безопасности // Интеграл» 2013. № 5,6. С. 54–57.

7. *Сашников Т.К.* К вопросу организации динамического мониторинга состояния информационной безопасности с использованием гибридных нейронечётких сетей // Интеграл. 2013. № 5,6. С. 34–36.

## ON THE APPLICATION OF FUZZY PRODUCTION MODELS IN THE SUBSYSTEMS OF INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS FOR SPECIAL PURPOSES

**Klyanchin Valery Konstantinovich,** Penza, Russia, atlas@sura.ru
**Sashnikov Timur Kasimovich,** Penza, Russia, *atlas@sura.ru*

**Abstract**
Information and communication resources of the automated control systems for special purposes are currently being increasingly numerous malicious attacks. This factor creates a serious threat for national defense and security of its citizens. In this regard, the development of subsystems of information security of the critical technical systems, one of the main tasks is to ensure the necessary level of quality protection of information resources, taking into account the specific conditions of operation, the requirements to combat constantly improving destructive attempts to influence offenders of different levels of training and equipping of and implementation opportunities for effective functioning in a dynamically changing environment. Quality improvement is fundamentally important properties of subsystems of information security is increasingly associated with the active application of intelligent data processing. This innovative approach provides an opportunity to use when creating the latest information security technology based on the extraction and processing of knowledge. Considered concept is based on an architecture consisting of the following structural components: expert subsystem, telecommunications environment, a subsystem of information safety, operating environment, a knowledge base currency discrete data into knowledge. The sources of knowledge about the subject area be both practical experience of experts and information during monitoring the external environment and internal sources. Knowledge is represented in the form of fuzzy production rules, which can be processed together with the input data using a production apparatus for fuzzy inference. As an example showing the specific mechanisms for the implementation of ideological approaches to the use of artificial neural networks and fuzzy logic. The problems of fuzzy rules extraction from digital data on the basis of known techniques, one of which is presented in the article. By using the proposed concept of building information security system it is possible to create the security of information systems with new possibilities in terms of interface interaction with the experts, taking into account the experience, adaptation to change, evolutionary development, in combination helps to ensure effective protection of information systems.
**Keywords:** automated control system; information security; expert system; base of fuzzy rules; production rules; fuzzy inference; fuzzy sets; membership function; fuzzification; artificial neural network.

**References**
1. Borodakiy Y. Forward-looking information protection system must be smart. Information Security. INSIDE. 2013. No. 2. Pp. 48–51. (In Russian)
2. Abraham A., Semchenko P. Rule-based expert systems. Scientists note of Pacific ocean states university. 2014. Vol. 5. No. 4. Pp. 1249–1266. (In Russian)
3. Rutkovskaya D., Pilinsky M., Rutkowski L. Neural networks, genetic algorithms and fuzzy systems. Moscow, Hotline — Telecom. 2007. 452 p. (In Russian)
4. Borisov V., Kruglov V. Fedulov A. Fuzzy model and network. Moscow, Hot line-Telekom. 2012. 284 p. (In Russian)
5. Sashnikov T. On the question of the application of data mining techniques in information security technologies of mobile communication systems. Proceedings of the XVIII International Scientific Conference "Innovation 2013". Moscow. Energoatomizdat. 2013. Pp.132–134. (In Russian)
6. Sashnikov T. About application of soft computing for the solution of the information security problems. Integral. 2013. No. 5, 6. Pp. 54–57. (In Russian)
7. Sashnikov T. About dynamical monitoring of the state of information security with hybrid neuro fuzzy network. Integral. 2013. No. 5, 6. Pp. 34–36. (In Russian)

**Information about authors:**
Klyanchin V.K., Director of Penza branch of Federal state owned unitary enterprise "STC "ATLAS";
Sashnikov T.K., Deputy Director of Penza branch of Federal state owned unitary enterprise "STC "ATLAS".

# ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ ЗАЩИЩЁННОСТИ СИСТЕМЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

**Гаврилов Илья Вячеславович,**
*сотрудник Академии ФСО России, г. Орёл, Россия, ilya_vch@pisem.net*

**Аннотация**
Необходимость в защите большого объёма речевой информации в различных государственных и коммерческих организациях в условиях стремительного роста возможностей технических средств перехвата информации по различным техническим каналам утечки определяет применение комплекса средств защиты, обладающих различной надёжностью. Поэтому возникает задача исследования влияния надёжности элементов технических систем защиты на защищённость речевой информации, циркулирующей в таких системах. Для решения задачи была определена структурно-функциональная модель системы защиты речевой информации, отмечено влияние технического состояния средств защиты на защищённость речевой информации в случае необходимости использования средств защиты, получен вариант для расчёта показателя защищённости системы защиты, отражена связь показателей надёжности средств защиты с показателями защищённости системы. В материалах представлены механизмы подсчёта показателей надёжности при учёте состояния средств защиты, составляющих комплексную систему. Результаты исследования показали необходимость комплексной оценки защищённости речевой информации.

**Ключевые слова:** *речевая информация; словесная разборчивость; каналы утечки информации; средства активной защиты; надёжность технических систем.*

В настоящее время речь является наиболее важным способом человеческого общения. Объёмы информационных потоков современного мира постоянно нарастают. Также растёт и ценность информации, что заставляет обладателей информации задумываться о её защищённости. Речь является основой при взаимодействии начальников и подчинённых любого уровня.

В соответствии с ГОСТ 512752006 к факторам, воздействующим на безопасность защищаемой информации в частности относятся:

- передача сигналов по проводным, опто-волоконным линиям, в оптическом и диапазоне радиоволн;
- излучения акустических и электромагнитных сигналов;
- побочные электромагнитные излучения;
- различные паразитные электромагнитные излучения;
- наводки в различных цепях и линиях связи;
- акустоэлектрические преобразования;
- дефекты, отказы оборудования.

И поэтому возможности потенциального противника по перехвату информации на современном этапе развития не ограничиваются разрозненным слежением за отдельными каналами утечки информации. Съём информативных сигналов осуществляется интегрировано сразу по нескольким каналам с последующим анализом и объединением полученных данных.

Вследствие чего возникает необходимость комплексного подхода к построению системы активной защиты речевой информации.

В рамках исследования разработана структурно-функциональная модель системы защиты речевой информации, которая включает источник речевой информации (ИРИ), основные и вспомогательные технические средства обработки информации [1], возможные технические каналы утечки речевой информации (ТКУРИ) [1, 2] со средствами активной защиты (САЗ) [1], среда распространения и злоумышленник с комплексом технических средств разведки. Функциональная зависимость сигналов, проходящих по различным каналам к злоумышленнику показана формулами (1)–(5).

$$A(t)=F_a[A_{ос}(t), A_{ш}(t), n_a(t)] \quad (1)$$

$$V(t)=F_v[V_{ос}(t), V_{ш}(t), n_v(t)] \quad (2)$$

$$P(t)=F_p[P_{ос}(t), P_ш(t), n_p(t)] \quad (3)$$

$$U(t)=F_l[U_{ос}(t), U_ш(t), n_l(t)] \quad (4)$$

Здесь условно обозначены функционалы от временной функции опасного сигнала, шума САЗ, естественных помех по акустическому (1), виброакустическому (2), визуально-оптическому (5) каналам, в радиоэфире (3) и в токопроводящих конструкциях (4).

При рассмотрении представленной структурно-функциональной модели необходимо отметить, что функционирующие в системе защиты САЗ участвуют в формировании сигнала, поступающего к злоумышленнику, который содержит «следы» информативного сигнала. Очевидно, что корректная работа САЗ непосредственно влияет на защищённость речевой информации, которая таким образом будет определяться надёжностью САЗ. Данные факты можно продемонстрировать с помощью следующих примерных графиков.

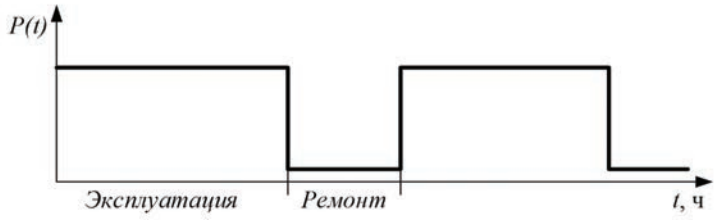



**Рис. 1.** Подход к определению надёжности САЗ на стадиях жизненного цикла в настоящее время

В настоящий момент существует устаревший подход к определению показателей надёжности САЗ (например, вероятности безотказной работы). Считается, что на протяжении всего периода эксплуатации САЗ данные показатели неизменны (рис. 1).

В реальности же в процессе эксплуатации вероятность отказов возрастает, а вероятность безотказной работы снижается по некоторому закону (рис. 2).

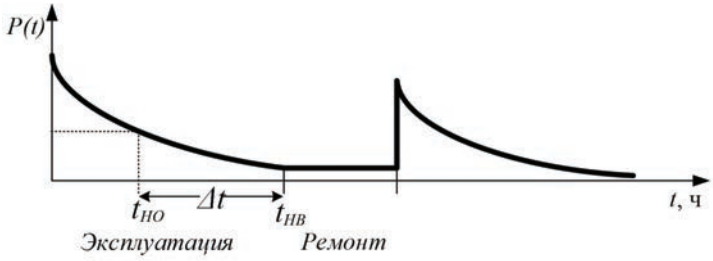



**Рис. 2.** Подход к определению надёжности САЗ на стадиях жизненного цикла в настоящее время

Это приводит к возрастанию интенсивности отказов, что с момента времени t начала отказа (на графике *t* начала отказа до этапа восстановления работоспособности) может характеризоваться утечкой речевой информации.

Поэтому актуальность проводимого исследования определяется необходимостью разрешения противоречия между существующим предположением о постоянном уровне надёжности системы активной защиты на периоде эксплуатации и реальном факте снижения показателей надёжности САЗ в процессе эксплуатации.

В данном исследовании выдвинута гипотеза о повышении защищённости речевой информации при поддержании структурной надёжности системы активной защиты. Под структурной надёжностью системы защиты будем понимать свойство системы активной защиты речевой информации, состоящее в её способности выполнять функции по защите речевой информации, сохраняя при этом основные характеристики вырабатываемых шумовых помех в пределах, необходимых для обеспечения снижения общего по всем техническим каналам уровня словесной разборчивости до значения, не позволяющего восстановить исходную информацию.

Целевая функция исследования в виде функционала представлена формулой (6).

$$\begin{cases} P_{ЗРИ} = F(W_{ОРИ}, \Delta F_i, \dfrac{P_{ci}}{P_{ші}}, \Lambda_i(T^\circ, p, \gamma), t_{HBi}, G, C) \xrightarrow{G} \max \\ W_{ОРИ} \le W_{пред} \\ C \le C_{доп} \end{cases}, \quad (6)$$

где РЗРИ — вероятность защиты речевой информации

*WЗРИ* — общая словесная разборчивость речевых сообщений у злоумышленника

$\Delta F_i$ — полоса частот *i*-го маршрута прохождения сигнала от ИРИ к злоумышленнику

$\Lambda_i(T^\circ, p, \gamma)\ \dfrac{P_{ci}}{P_{Hi}}$ — отношение сигнал/шум для *i*-го маршрута;

— *i*-й показатель надёжности, зависящий от факторов окружающей среды;

$t_{HBi}$ — время начала восстановительных мероприятий для *i*-го маршрута;

*G* — матрица структуры графа системы активной защиты речевой информации;

*C* — затраты на внедрение и эксплуатацию средств защиты;

$W_{пред}$ — значение предельно допустимой словесной разборчивости перехватываемого по каналам утечки информации речевого сообщения;

$C_{доп}$ — допустимые затраты на внедрение и эксплуатацию средств защиты.

Приняв во внимание факт использования злоумышленником для получения речевой информации цифровые устройства и методы восстановления цифровой информации, можно заключить, что параметры возникающих каналов утечки информации хорошо описываются с помощью предела пропускной способности Шеннона [3] для *i*-го непрерывного канала утечки информации [2] с помощью формулы (7).

$$C_i' = \Delta F_i \cdot \log_2\left(1 + \frac{P_{ci}}{P_{Hi}}\right) \tag{7}$$

Защищённость речевой информации определяется значением словесной разборчивости [2], которую, исходя из преобразования речевой информации в цифровую форму можно выразить формулой (8):

$$W_{ОРИ} = \frac{\sum_i I_{зi}}{I_{ИРИ}}, \tag{8}$$

где $I_{зi} = C_i' \cdot \Delta t_i$ — количество информации, полученной злоумышленником по *i*-му маршруту;

$\Delta t_i = t_{НВ} - t_{НО}$ — время, в течение которого функционирует *i*-ый комплект неработоспособных САЗ с вероятностью безотказной работы ниже определённого порогового уровня (рис. 2);

$t_{НВi}$ — время начала восстановления САЗ;

$t_{НОi}$ — время начала отказа САЗ;

$I_{ИРИ}$ — количество информации, порождаемое ИРИ за время $\Delta t$.

Полагая в качестве примера, что величина $P(t)$ распределена по экспоненциальному закону [4], можно выразить $t_{HOi}$ через интесивность отказов $\Lambda$, получив формулу (9) для общей словесной разборчивости:

$$W_{ОРИ} = \frac{\sum_i \left[ \Delta F_i \cdot \log_2\left(1 + \frac{P_{ci}}{P_{ши}}\right) \cdot \left( t_{HBi} + \frac{\ln P_{пор}}{\sum_{j=1}^{N} \left( \lambda_j \cdot \alpha_{jм} \cdot \alpha_{jt} \cdot \alpha_{jB} \cdot \alpha_{jД} \cdot K_{jH} \right)} \right) \right]}{I_{ИРИ}} \tag{9}$$

где $\lambda_i$ — интенсивность отказа элемента САЗ в нормальных условиях эксплуатации;

$\alpha_{iм}$ — коэффициент, учитывающий влияние на надежность элемента САЗ механических воздействий;

$\alpha_{iB}$ — коэффициент, учитывающий влияние на надежность элемента САЗ влажности;

$\alpha_{iД}$ — коэффициент, учитывающий влияние на надежность элемента САЗ давления;

$K_{iH}$ — коэффициент электрической нагрузки, учитывающий особенности функционирования принципиальной схемы с выбранными элементами.

Исходя из цели исследования, необходимо повысить защищённость речевой информации от утечки по техническим каналам посредством обеспечения структурной надёжности системы активной защиты. Структура системы активной защиты задаётся матрицей G, в которой определяется расположение элементов системы, а также их показатели надёжности. Вероятность защиты речевой информации рассчитывается, исходя из формул (2) и (3). Где вероятность утечки характеризуется вероятностью наступления события, при котором общая словесная разборчивость на стороне злоумышленника будет выше предельно допустимой по нормативным документам.

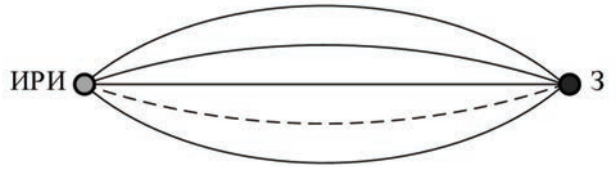



**Рис. 3.** Граф возможных ТКУРИ

В настоящей работе предложено использовать подходы теории графов [5] для моделирования системы активной защиты речевой информации. На рис. 3–6 показан переход от графа возможных ТКУРИ к графу структурной надёжности системы активной защиты.

На данных рисунках применяются следующие обозначения:

$G = (V, E)$ — ориентированный граф ТКУРИ;

$V = \{v_{ИРИ}, v_з, v_{11}, v_{12}, \ldots, v_{1N\_1}, v_{21}, v_{22}, \ldots, v_{1N\_2}, \ldots, v_{M1}, v_{M2}, \ldots, v_{MN\_M}\}$ — множество вершин (преобразователи сигналов между средами и ретрансляторы);

$v_{ИРИ}$ — источник речевой информации;

$v_з$ — злоумышленник;

$E = \{e_{11}, e_{12}, \ldots, e_{1N\_1+1}, e_{21}, e_{22}, \ldots, e_{2N\_2+1}, \ldots, e_{M1}, e_{M2}, \ldots, e_{MN\_M+1}\}$ — множество дуг (среды распространения сигналов).

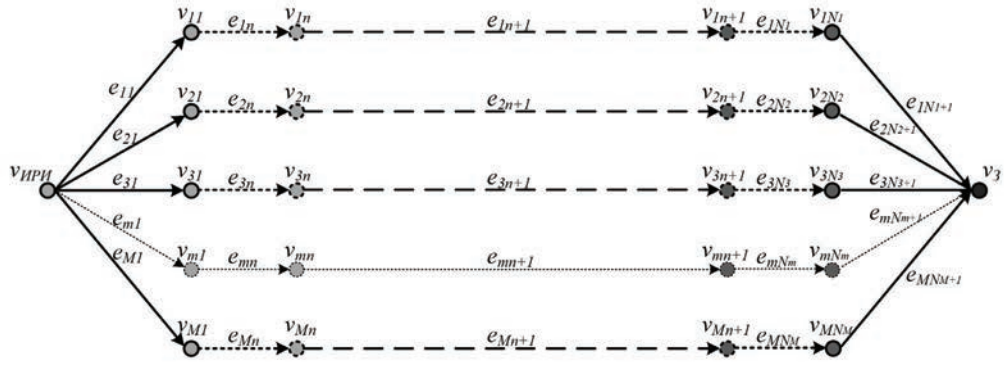


**Рис. 4.** Детализированный граф возможных ТКУРИ

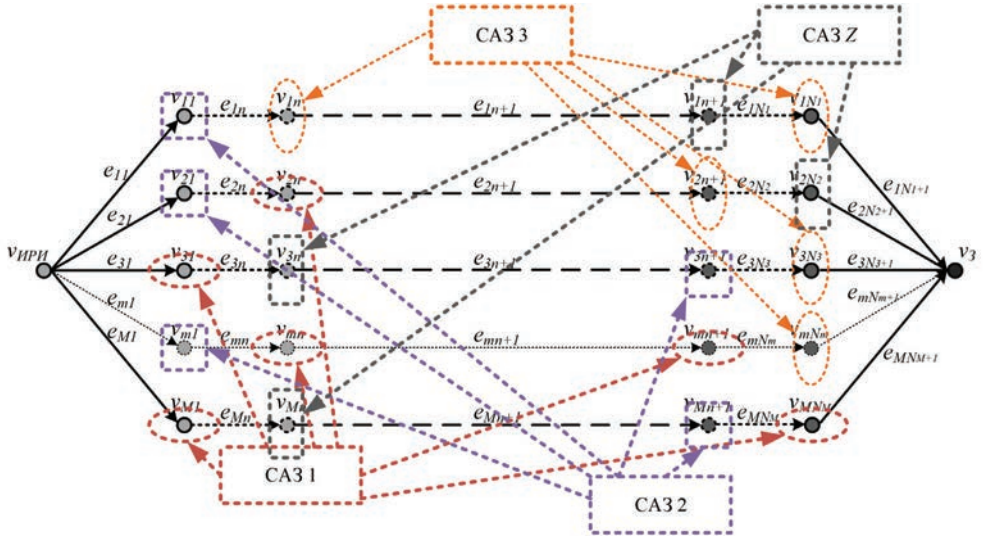



**Рис. 5.** Детализированный граф возможных ТКУРИ при активном шумовом воздействии

**Рис. 6.** Граф структурной надёжности системы активной защиты

Математическое выражение для расчёта показателей структурной надёжности системы активной защиты представлено формулой 10.

$$W(G)=1-\prod_{m\in M}\left[1-W_m\left(n_m,M_m\right)\right]=1-\prod_{m\in M}\left[1-\prod_{v_m\in v_{MN_m}}W_m\left(v_m\right)\cdot W_{mn}\left(e_{mn}\right)\right] \quad (10)$$

В результате исследования получены следующие графики зависимости вероятности защиты информации от времени эксплуатации (рис. 7):

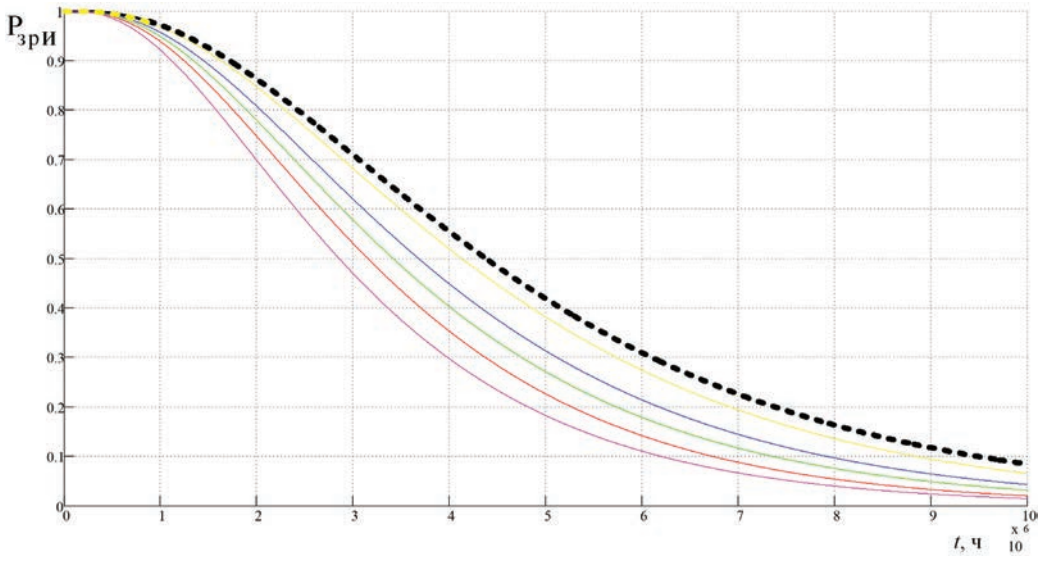



**Рис. 7.** Семейство графиков зависимостей вероятности защиты речевой информациионт времени работы комплекса САЗ при различном количестве равнонадёжных САЗ

В случае учёта комплексного характера утечки речевой информации наблюдается повышение словесной разборчивости, а значит снижение защищённости речевой информации.

Исследования показывают необходимость комплексной оценки защищённости речевой информации.

**Список литературы**

1. *Бузов Г. А., Калинин С. В., Кондратьев А. В.* Защита от утечки информации по техническим каналам. М.: Горячая линия — Телеком. 2005. 416 с.

2. *Железняк В. К.* Защита информации от утечки по техническим каналам. ГУАП. СПб. 2006. 188с.

3. *Прокис Д.* Цифровая связь. Пер.с англ. / Под ред. Д. Д. Кловского. М.: Радио и связь. 2000. 800 с.

4. *Боровиков С. М., Цырельчук И. Н., Троян Ф. Д.* Расчёт показателей надёжности радиоэлектронных средств / под ред. С. М. Боровикова. Минск: БГУИР. 2010. 68 с.

6. *Курносов В. И., Лихачёв А. М.* Методология проектных исследований и управление качеством сложных технических систем электросвязи. СПб.: ТИРЕКС, 1998. 496 с.

## FEATURES DEFINITIONS OF PROTECTED PARAMETERS OF SECURITY STSTEM OF SPEECH INFORMATION

**Gavrilov Ilya Vyacheslavovich,**
*Orel, Russia, ilya_vch@pisem.net*

**Abstract**

The need to protect the small amount of voice data in a variety of government and commercial organizations in the face of rapid growth in capacity of means of interception of information on various technical channels of leakage defines the use of complex remedies have varying reliability. Therefore, there is the problem of investigating the influence of changes of elements of technical security systems on a secure voice information circulating in these systems. To solve the problem was identified structural and functional model of the system of protection of speech information, noted the influence of the technical state of protection to a secure voice information in the event of the need for protection, obtained an option to calculate the index of security protection system reflects the relationship indicators of reliability of protection with indicators of security system. The documents show the mechanisms of reliability indicators calculation by taking into account the state of protection, constitute a complex system. The results showed the need for a comprehensive assessment of security of voice data.

**Keywords:** *voice information; speech recognition; information leakage; the active means of protection; reliability of technical systems.*

**References**

1. Buzov G.A., Kalinin S.V., Kondrat'ev A.V. Protection against information leakage on technical channels. Moscow: Telekom. 2005. P. 416. (In Russian)
2. Jeleznyak V.K. Protection against information leakage on technical channels. St-Petersburg. 2006. 188p. (In Russian)
3. Prokis D. Digital communication. Ed. D.D. Klovskogo. Moscow: Radio i svyaz'. 2000. 800 p. (In Russian)
4. Borovikov S.M., Calculation of reliability indicators of radio-electronic means. under edition. Minsk, BGUIR, 2010. 68 p. (In Russian)
5. Kurnosov V.I., Lihachev A.M. Methodology of design researches and quality management of difficult technical systems of telecommunication. . St. Peterburg, TIREKS, 1998. 496 p. (In Russian)

**Information about author:**
*Gavrilov I.V., assistant, Academy of Federal Agency of Protection of Russian Federation.*

# ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ УПРАВЛЕНИЯ ФУНКЦИОНАЛЬНОСТЬЮ МОБИЛЬНЫХ УСТРОЙСТВ НА БАЗЕ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

**Разумов Антон Николаевич,**
*сотрудник академии Федеральной службы охраны России, г. Орёл, Россия,*

**Маркин Дмитрий Олегович,**
*сотрудник академии Федеральной службы охраны России, г. Орёл, Россия, admin@nikitka.net*

**Аннотация**
Современные мобильные абонентские устройства представляют собой практически универсальные медиаустройства с серьезными вычислительными возможностями и способностями предоставлять исчерпывающее количество услуг пользователю. Данный факт приводит к желанию пользователей использовать такие устройства, как для личных целей, так и для выполнения служебных обязанностей. Однако использование мобильных устройств в корпоративной среде, содержащей конфиденциальные сведения, порождает ряд проблем с точки зрения безопасности информации. При этом существующие системы управления мобильными устройствами не всегда способны обеспечить безопасность информации на должном уровне при доступе к ним пользователей с использованием мобильных устройств. В работе проведен анализ состава, функциональных возможностей и особенностей обеспечения безопасности информации при работе с мобильными устройствами. Исследованы актуальные факторы, воздействующие на безопасности информации в корпоративной среде, содержащей конфиденциальные сведения, при работе в ней пользователей мобильных устройств. Представлены модели угроз и нарушителя информационной безопасности при работе с мобильными устройствами. На основе проведенного анализа факторов, моделей угроз и нарушителя, сформированы предложения по составу средств защиты информации для обеспечения безопасности информации при доступе к информационным ресурсам с использованием мобильных устройств. Предложен способ управления функциональными возможностями мобильного устройства в зависимости от его местоположения и требований безопасности, установленных в организации, позволяющий обеспечить конфиденциальность информации при доступе к информационным ресурсам защищенной корпоративной сети.

**Ключевые слова:** *мобильные абонентские устройства; управление доступом; управление функциональностью; обеспечение конфиденциальности; защита от утечки информации.*

За последние годы наблюдается бурный рост популярности мобильных устройств. По прогнозам аналитических агентств [1] к 2016 году почти половина эксплуатируемых в организациях устройств будет относиться к мобильным. Причиной такой популярности мобильных устройств в первую очередь является увеличение их производительности и функциональных возможностей, что ведет к повышению возможностей работы с корпоративными информационными ресурсами организации. Однако использование мобильных устройств в корпоративной среде с конфиденциальной информации в настоящее время ограничено, поскольку существующие средства защиты информации не позволяют обеспечить конфиденциальность информации при доступе к ней пользователей с использованием мобильных устройств. Отсутствие таких средств защиты создает технические каналы утечки конфиденциальной информации, увеличивает возможности нарушителей по несанкционированному доступу, подмене или компрометации важных данных.

Для обеспечения необходимого уровня конфиденциальности информации в организации мобильные устройства, в частности, смартфоны и планшеты, должны соответствовать требованиям в области информационной безопасности: обеспечивать конфиденциальность, целостность и доступность данных (ГОСТ Р 50922–2006. Защита информации. Основные термины и определения).

В настоящее время существует ряд технических решений, позволяющих управлять некоторыми функциональными возможностями мобильных устройств на основе установленной политики безопасности организации. Такими решениями являются так называемые системы управления мобильными устройствами Mobile Device Management (MDM). Они представляют собой систему функций по защите и управлению данными и приложениями на мобильном устройстве. MDM является

важным компонентом всего жизненного цикла мобильных устройств, включающим аппаратное обеспечение, программное обеспечение и техническое сопровождение этих устройств в ходе их эксплуатации. В условиях все большего вовлечения смартфонов и планшетов в процессы организаций управление мобильными устройствами становится важнейшей задачей при этом необходимо определить какими существенными параметрами мобильного устройства необходимо управлять, чтобы обеспечить конфиденциальность информации при доступе к ней с использованием данных устройств.

Современный мобильный телефон представляют собой медиаустройство для повседневной работы и развлечений, где функция телефонных переговоров не является первостепенно важной. Это отражено и в перемене названия мобильного телефона — смартфон, коммуникатор, фаблет и др. В результате технической эволюции функциональная и структурная организация такого устройства в настоящее время представляет собой малогабаритный компьютер со своей операционной системой, центральным процессором, оперативной памятью и специфическими устройствами ввода-вывода [22].

К основным **базовым аппаратным и программным параметрам мобильных устройств**, влияющим на безопасности информации, относятся:

- габаритные размеры;
- интерфейсы для сетевого доступа, поддерживающие стандарты GSM 900/1800/1900, 3G, 4G LTE;
- встроенное и схемное хранилище данных;
- функции для удаленной синхронизации данных (email, облачные хранилища данных);
- поддержка сетевых служб;
- навигационная система, предлагающая сервисы определения местоположения (GPS, ГЛОНАСС, Beidou);
- интерфейсы Wi-Fi 802.11n, Bluetooth 4.0, USB, NFC;
- мультимедийные возможности (камера, встроенные динамик и микрофон).

Наличие данных параметров у мобильных устройств определяет совокупность **факторов, воздействующих на безопасность защищаемой информации**. Согласно нормативным документам (ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.) и с учетом указанных параметров мобильных устройств были выделены актуальные факторы, определяющие наличие угроз информационной безопасности мобильного устройства, к которым относятся:

1. Внутренние:

- передача информации по открытым каналам связи;
- копирование информации на незарегистрированный носитель;
- несанкционированное копирование информации.

2. Внешние:

несанкционированный доступ к защищаемой информации путём подключения к техническим средствам и системам обработки информации;

- хищение носителя информации;
- сетевые атаки;
- несанкционированное использование программного обеспечения средств обработки защищаемой информации.

Указанные факторы определяют **актуальные угрозы безопасности при работе с мобильными устройствами**. Основными угрозами, включающими в себя определение соответствующих ресурсов, уязвимостей и параметров безопасности в отношении этих ресурсов, являются:

- угроза выявления паролей;
- угроза получения НСД путём подмены доверенного объекта;
- угроза потери (кражи) мобильного устройства;
- угроза использования запрещённых приложений;
- угроза использования открытых сетей;
- угроза разглашения защищаемой информации;
- угроза воздействия на средства управления конфигурации мобильного устройства;
- угроза нарушения функционирования функциональных модулей мобильного устройства;
- угроза перехвата обрабатываемых данных;
- взаимодействие с другими системами;
- угроза использования непроверенного контента;
- использование служб определения местоположения.

Указанный перечень угроз, а также факторы, воздействующие на безопасность информации, позволяют определить **возможности нарушителей информационной безопасности при работе с мобильными устройствами**. Благодаря вышеперечисленным факторам и угрозам безопасности нарушитель может получить несанкционированный доступ к сведениям организации, а также нанести деструктивное воздействие, выраженное в нарушении конфиденциальности, целостности и доступности.

Ниже представлена характеристика состава возможных нарушителей и их возможности по реализации угроз безопасности информации:

1. Внешние нарушители:
– бывший сотрудник организации может реализовать угрозы: а, б, в, и;
– посторонние лица, пытающиеся получить доступ к данным, могут реализовать угрозы: ж, з, и;
– представители преступных организаций могут реализовать угрозы: а, ж, з, и.
2. Внутренние нарушители:
– сотрудники организации могут реализовать угрозы: а, б, в, г, д, е;
– пользователи, имеющие ограниченный доступ к данным, могут реализовать угрозы: в, г, е;
– пользователи, осуществляющие удалённый доступ, могут реализовать угрозы: д, и;
– пользователи с полномочиями администратора могут реализовать угрозы: ж.

На основании представленных потенциальных возможностей нарушителей сформирован **перечень требований безопасности**, которые должны выполняться при доступе к информационным ресурсам защищенной корпоративной сети с использованием мобильных устройств. К этим требованиям относятся:
– реализация механизма ограничения доступа к аппаратным и программным ресурсам мобильного устройства;
– автоматический мониторинг и детектирование состояния программно-аппаратной среды мобильного устройства;
– обеспечение криптографической защиты конфиденциальных данных при их передаче и хранении;
– контроль содержания оперативной памяти устройства, а также наличие возможности дистанционного удаления информации из памяти устройства в случае его утери или кражи;
– аутентификация устройства и его пользователя;
– наличие изолированной программной среды;
– управление доступом к информационным ресурсам;
– ограничение доступа пользователей и приложений к аппаратным средствам, таким как цифровая камера, GPS, интерфейс Bluetooth, интерфейс USB и съемные носители;
– ограничение доступа пользователей и приложений к функциям операционной системы, таким как встроенный web-браузер, почтовый клиент, календарь, контакты, службы установки приложений;
– менеджмент беспроводных сетевых интерфейсов (Wi-Fi, Bluetooth);
– автоматизированный контроль исполнения политик, обнаружение и протоколирование случаев их нарушения, таких как изменение утвержденной базовой конфигурации безопасности, и автоматическое принятие мер, когда это возможно и целесообразно;
– ограничение или запрет доступа к корпоративным сервисам на основе информации о версии и состоянии операционной системы мобильного устройства, о производителе, марке, модели, или версии клиентского приложения.

Реализация данных требований возможна при наличии централизованного управления мобильными устройствами организации, предполагающего постоянный мониторинг состояния мобильных устройств в организации и формирование на основе мониторинга — управляющих воздействий в виде назначаемых мобильным устройствам конфигураций и прав доступа пользователям.

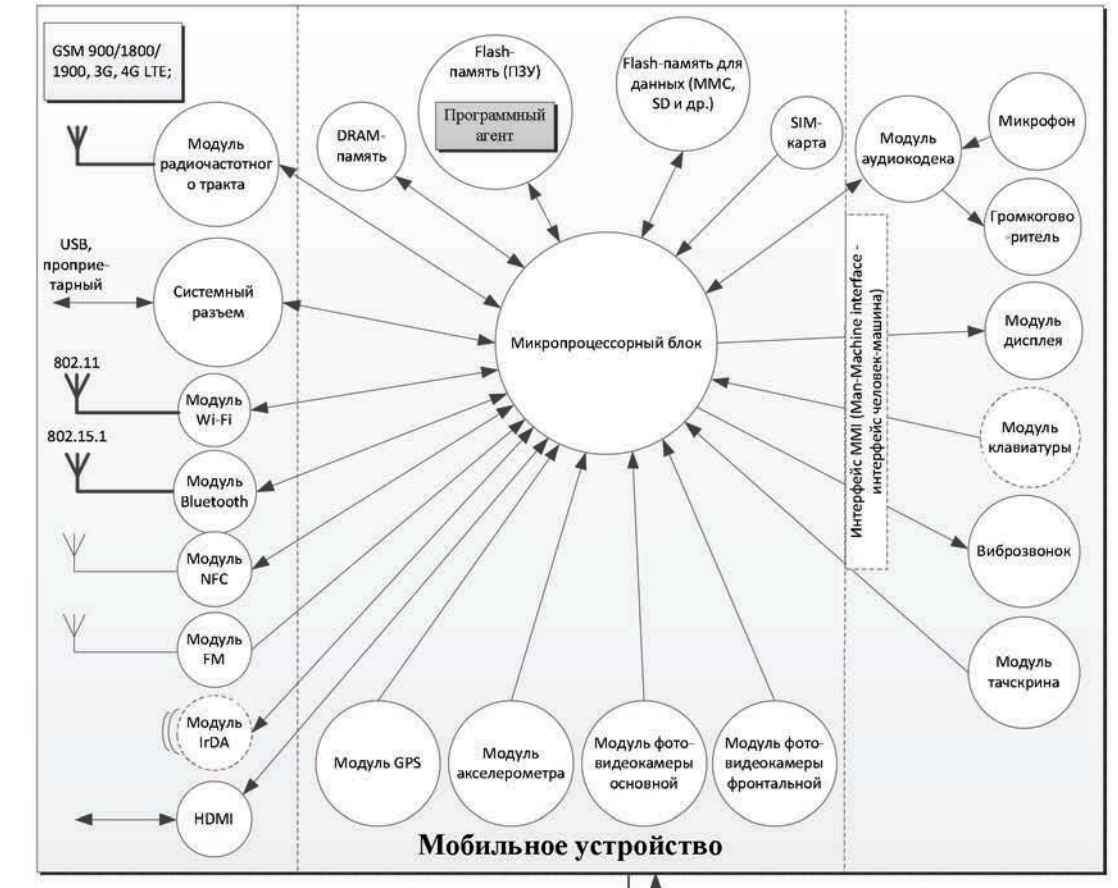
В настоящее время существуют готовые **программно-технические решения, осуществляющие управление мобильными устройствами** в корпоративной среде. Примером таких программ являются SOTI Mobicontrol, Mobile Device Management, SAP Afaria, MobileIron MyPhone@Work, AirWatch MDM, Junos Pulse Mobile Security Suite, Kaspersky Security. Однако анализ [3] их функциональных возможностей показал, что у данных средств присутствуют недостатки:
– иностранное производство и закрытый программный код;
– отсутствие сертификации у регуляторов;
– отсутствие интегрированных подсистем определения местоположения мобильных устройств в зданиях с точностью до помещений.

Система управления мобильными устройствами может быть построена на основе клиент-серверной архитектуры, в которой элементом, отвечающим за исполнение управляющих команд на стороне мобильного устройства, может являться программно-аппаратный модуль, интегрированный на плате мобильного устройства либо программный агент, реализующий управление функциональностью мобильного устройства.

Функциями такого программного агента является:
– удаленное конфигурирование устройств (настройки Wi-Fi, Bluetooth, сетевой модуль);
– удаленная инвентаризация устройств для контроля их соответствия корпоративным политикам и стандартам;
– прекращение доступа к корпоративным приложениям для тех пользователей, которые покинули компанию;
– определение местоположения мобильного устройства;
– сбор статистики об используемых услугах;
– удаленная блокировка устройства (с удалением информации на нем) в случае потери или кражи устройства.

**Реализация программного агента** удаленного управления функциональностью мобильного устройства может быть выполнена на базе операционной системы (ОС) Android. Современные версии данной операционной системы при условии установки приложения в качестве администрирующего предоставляет широкие возможности для программного управления параметрами мобильного устройства. Таким образом, используя клиент-серверную архитектуру на базе про-

граммного агента в виде приложения для ОС Android и удаленного веб-сервера, выполняющего роль управляющего, можно реализовать предлагаемую систему управления мобильными устройствами. Структурная схема, реализующая взаимосвязь мобильного устройства и удаленного сервера доступа мобильных устройств, представлена на рис. 1.




**HTTP-запрос** (атрибуты доступа):
1) данные о местоположении (CellID, геокоординаты);
2) ID устройства, ОС, прикладного ПО;
3) информация о процессах.
4) ...

**HTTP-ответ** (конфигурация МУ):
1) перечень разрешенных/запрещенных функций
2) перечень разрешенных/запрещенных приложений
3) ...


| Конфигурация | Местоположение | Атрибуты доступа | | | |
|---|---|---|---|---|---|
| | | Время | ID УМУ | User | ... |
| $CONF_0$ | $\Gamma(L_O \vee L_{K1} \vee L_{K2})$ | ∞ | ∞ | ∞ | ... |
| $CONF_1$ | $L_O$ | ∞ | 5,29,53,... | 3,7,12,... | ... |
| $CONF_2$ | $L_O$ | $8^{00}$-$17^{30}$ | 7,11,52,... | 9,17,23,.. | ... |
| $CONF_3$ | $L_{K1}$ | ∞ | 13,17,... | 5,11,... | ... |
| $CONF_4$ | $L_{K1}$ | $16^{00}$-$17^{00}$ | 17 | 5 | ... |
| $CONF_5$ | $L_{K2}$ | ∞ | 13 | 1 | ... |
| $CONF_6$ | $L_{K2}$ | $11^{00}$-$13^{00}$ | 17,21 | 11,27 | ... |

**Рис. 1.** Структурная схема, реализующая взаимосвязь мобильного устройства и удаленного сервера доступа мобильных устройств

В состав мобильного устройства входят группа функциональных модулей для ввода-вывода информации, вычислительный блок, блок датчиков, блок устройств хранения информации.

Для реализации требований безопасности защищенной корпоративной сети предусмотрена табулированная функция, содержащая взаимосвязь параметров, характеризующих условия функционирования мобильного устройства и его конфигурацию, удовлетворяющую требованиям безопасности для текущих условий.

Канал управления между мобильным устройствам и удаленным сервером доступа может быть организован на базе защищенного HTTPS соединения.

HTTP-запрос передаёт удаленному серверу текущие условия и состояние мобильного устройства. Такие сведения могут включать в себя: идентификатор устройства, имя и другие служебные атрибуты, необходимые для управления функциональностью аппарата. Пример такого HTTP-запроса представлен ниже:

```
https://api.mdac.php?device_name=YOTAPHONE&device_id=YA454-45-5-45&attri-
butes=1010001111&GEO_info=46.757;57.5786
```

Удалённый сервер-доступа в таком случае должен состоять из веб-сервера, базы данных и прикладного программного обеспечения (веб-приложения), обрабатывающего запросы от мобильных устройств. В ответ на полученный HTTP-запрос данное приложения обрабатывает входящие в него данные об условиях функционирования устройства, включающие в том числе геоинформацию о его местоположении, и формирует команду для исполнения мобильному устройству. Данная команда формируется из директив на включение/выключение функциональных блоков мобильного устройства, а также команд для исполнения на стороне мобильного устройства определенных заданных действий. Пример HTTP -ответа приведён ниже:

```
Wi-Fi=1;Bluetooth=0;MobileData=1;Command=1010111
```

Целесообразно канал управления между мобильным устройством и удаленным сервером доступа реализовать защищенным с установлением VPN-канала. В случае, если разглашение местоположения пользователя мобильного устройства критично, могут быть использованы протоколы, реализующие конфиденциальные распределенные вычисления, такие как «Забывчивая передача» [5] или «Передача данных на хранение» [6].

Алгоритм работы:

Шаг 1. При получении служебной команды «stop» программный агент переходит в активное состояние. Начинается сбор статистики о текущем состоянии устройства, о статусе всех интерфейсов, а также определение текущего местоположения.

Шаг 2. При клиент-серверном обмене информацией на веб-сервер поступают данные с мобильного устройства.

Шаг 3. На основании полученных от мобильного устройства данных происходит сопоставление местоположения с данными в базе данных, после чего определяется политика безопасности для данного устройства.

Шаг 4. После успешного назначения политики безопасности формируются соответствующие команды для конфигурирования устройства в соответствии с задаваемыми требованиями плотики безопасности.

Шаг 5. При поступлении на устройство служебных команд (см. перечень служебных команд) происходит настройка функционала.

Шаг 6. Обмен http-обмен сообщениями происходит до отправки команды «stop» для постоянного контроля функционирования устройства в соответствии с заданными требованиями.

Шаг 6. При возникновении несоответствия алгоритм повторяется с шага 1.

Реализация описанной системы управления мобильными устройствами позволит снизить вероятность утечки конфиденциальной информации, и возможности нарушителей по несанкционированному доступу, подмене или компрометации важных данных за счет ограничения функциональности используемых в защищенной корпоративной сети мобильных абонентских устройств.

**Список литературы**

1. Развитие интернета в регионах России. Весна 2014 / Яндекс. Москва, 2014. URL: http://download.yandex.ru/company/ ya_internet_regions_2014.pdf. Дата обращения: 31.10.2014.

2. Хрусталев Д. А. Мобильные телефоны Siemens. Принципы устройства и ремонт. М.: Изумруд, 2004. 256 с.

3. Маркин Д. О., Комашинский В. В., Баранов И. Ю. Модель управления профилем защиты мобильного устройства при доступе к услугам с разным уровнем конфиденциальности // Информационные технологии. 2015. № 9 (21). С. 611–618.

4. Маркин Д. О., Комашинский В. В., Баранов И. Ю. Имитационное моделирование определения местоположения пользователей мобильных устройств внутри помещений // Информационная безопасность и защита персональных данных. Проблемы и пути их решения: матер. VII Межрегиональной научно-практическая конференция / под ред. О. М. Голембиовской. Брянск: БГТУ, 2015. С. 77–81.

5. Яковлев В. А., Шутый Р. С. Протокол «Забывчивая передача» с использованием интерактивного хэширования // Методы и техн. сред-ства обеспечения безопасности информации: матер. XVII Общерос. НТК. СПб.: Изд-во СПбГПУ, 2008. С. 74–75.

6. Яковлев В. А., Шутый Р. С. Модифицированный протокол «Передача бита на хранение» для канала с изменяемой вероятностью ошибки // Проблемы информационной безопасности. Компьютерные системы. 2008. № 1. С. 88–95.

## MOBILE DEVICES FUNCTIONALITY MANAGEMENT SYSTEM BASED ON ANDROID OPERATING SYSTEM

**Razumov Anton Nikolaevich**,
Oryol, Russia

**Markin Dmitriy Olegovich**,
Oryol, Russia, *admin@nikitka.net*

**Abstract**
Today mobile devises represent universal devices with great computing opportunities and abilities to provide number of services. This fact leads to users` desire to use such devices, both for the personal purposes, and for performance of official duties. However using mobile devices in the corporate environment containing confidential information generates a number of security problems. Thus the existing mobile device access control systems aren't capable to ensure safety of information. In this work the analysis of structure, functionality and secrecy information features during using mobile devices are presented. The actual factors influencing safety of information in the corporate environment containing confidential information are investigated. Threats model and information security violator model are presented. Using analysis of factors, threats and the violator models, the authors suggest mobile devices functionality management system structure to provide information access safety during using mobile devices. The method of mobile device functionality management depending on its location and safety requirements is offered. It is shown that such method allows to provide confidentiality of access to corporate confidential information using manage mobile devices.

**Keywords:** mobile devices; access control; functions management; confidence; information leakage protection.

**References**
1. Internet development in regions of Russia. Spring 2014. Moscow, 2014. URL: http://download.yandex.ru/company/ya_internet_regions_2014.pdf. Access Date: 31.10.2014. (In Russian)
2. Hrustalev D.A. Siemens mobile phones. Principles of the device and repair. Moscow : Izumrud, 2004. 256 p. (In Russian)
3. Markin D.O., Komashinskij V.V., Baranov I. Ju. Model upravlenija profilem zashhity mobilnogo ustrojstva pri dostupe k uslugam s raznym urovnem konfidencialnosti. Informacionnye tehnologii. 2015. No. 9 (21). Pp. 611-618. (In Russian)
4. Markin D.O., Komashinskij V.V. Imitating modeling of location determination of users mobile devices in rooms / Information security and protection of personal information. Problems and ways of their decision. Materialy VII Mezhregionalnoj nauchno-prakticheskaja konferencija. Ed. O. M. Golembiovskoj. Brjansk: BGTU, 2015. Pp. 77-81. (In Russian)
5. Jakovlev V.A., Shutyj R.S. The protocol "Forgetful transfer" with use of an interactive hashing. / Methods and means of safety of information. Metody i tehn. sred-stva obespechenija bezopasnosti informacii: Materialy XVII Obshheros. NTK. SPb, 2008. 74–75 p. (In Russian)
6. Jakovlev V.A., Shutyj R.S. The modified protocol "Bit transfer on storage" for the channel with changeable probability of a mistake. / Problems of information security. Computer systems. 2008. No. 1. Pp. 88–95. (In Russian)

**Information about authors:**
Razumov A. N., employer, Academy of Federal Guard Service of Russia;
Markin D. O., employer, Academy of Federal Guard Service of Russia.

# ПРЕДЛОЖЕНИЯ ПО РАЗРАБОТКЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ВОЗДЕЙСТВИЯ ИМИТАЦИОННЫХ ПОМЕХ НА КАНАЛЫ УПРАВЛЕНИЯ БПЛА В РЕЖИМЕ «ОЖИДАНИЕ»

**Иванов Роман Вячеславович,**
*лаборант 11 кафедры Военной академии связи имени С.М. Буденного,*
*г. Санкт-Петербург, Россия, demon13_84@mail.ru*

**Аннотация**
Обосновано, что техническое развитие систем кибернетики в значительной степени изменило облик ведения боевых действий и обусловило широкое использование беспилотных летательных аппаратов, которые играют значимую роль на поле боя, поэтому вопросы помехозащиты их каналов управления являются актуальными и значимыми как для разработчиков, так и специалистов, занимающихся эксплуатацией аппаратов.
Показано, что наибольшую опасность представляют структурные помехи, в связи с определенными трудностями их идентификации.
Указанные обстоятельства определяют актуальность разработки модели воздействия имитационных помех на каналы управления беспилотных летательных аппаратов в режиме «Ожидание», которая позволит выработать меры по борьбе с навязыванием ложных команд и нарушениями функционирования приемной аппаратуры.
В работе проанализированы особенности режима «Ожидание» с позиций возможных состояний аппаратуры. Описано геометрическое пространство существования доступных сигналов. Обосновано его многомерность, причем отдельно выделена сигнатурная составляющая векторов состояний сигнала, как их определяющий признак. Представлено и описано частотно-сигнатурно-временное состояние канала управления (телеметрической системы) с позиций области его допустимых значений. С учетом рассмотренной методологии определена вероятность наступления того или иного состояния канала как вероятностной меры пространства его допустимых значений.
Показано, что по аналогии с системами криптографической защиты, наибольший уровень неопределенности возникает в том случае, если изменение состояний канала происходит по равномерному закону, поскольку в этом случае обеспечивается максимальная имитационная защищенность. Только в таких условиях вероятность имитационного навязывания за одну попытку в пределах заданного времени определяется отношением числа состояний в единичном подпространстве к общему числу возможных состояний.
Для анализа последствий имитационного навязывания предложена модель, учитывающая особенности радиоканала управления в режиме «Ожидание» с учетом всех проанализированных факторов.
Обосновано, что процесс имитационного воздействия представляет собою последовательное многоразовое сканирование пространства состояний, представленного простейшим потоком Бернулли.
Показано, что оценка эффективности такого сканирования будет определяться посредством гипергеометрического распределения.
Определено результирующая оценка носит вероятностный характер и достижение конкретного заданного значения интерпретируется как вероятность обеспечения мероприятий по имитационной защите радиоканала, что позволяет для рассматриваемых условий и параметров связать ее значение с временем, необходимым для ее получения.

**Ключевые слова:** *математическая модель воздействия имитацитационных помех; канал управления БПЛА; геометрическое пространство сигналов.*

**Введение**

Новые способы ведения боевых действий предполагают широкое использование беспилотных летательных аппаратов (БПЛА). По своей сущности БПЛА является многофункциональным устройством, способным нести на себе как вспомогательное оборудование, так и летальное оружие. Учитывая, что размеры БПЛА достаточно малы, поразить их достаточно сложно, поэтому в качестве борьбы с ними применяют средства постановки помех.

Анализ возможностей средств РЭБ, состоящих на вооружении армии США, показал, что те способны ставить активные помехи в заградительном и прицельном режиме. Причем среди прицельных помех опасность представляют структурные, поскольку их применение может не только нарушить ход выполнения боевого задания БПЛА, но и привести к перехвату управления.

Между тем, вопросы борьбы с имитонавязыванием каналам управления БПЛА изучены достаточно слабо и на настоящий момент не существует четкого понимания какие меры необходимо принимать для снижения урона наносимого структурными помехами. Следовательно, для армии РФ существует реальная опасность, что в случае применяемые БПЛА могут не выполнить задание по предназначению.

Целью статьи является разработка модели воздействия имитационных помех на каналы управления БПЛА в режиме «Ожидание», которая позволит выработать меры по борьбе с имитонавязыванием системам управления.

**Теоретические основы построения модели**

Сущность имитонавязывания в режиме «Ожидание» состоит в подборе структуры помехи в соответствии с пространством существования сигнала радиоканала [1], которое факторизуем до уровня подпространств.

Для частотно-временного подпространства $\Omega_F \in (F_j, T_i), j = \overline{1,J}, i = \overline{1,\infty}$ факторизацию можно представить геометрически, при следующих условиях $\Delta F = \text{const}$; $\Delta T = T_{\text{см}} = \text{const}$ (где $T_{\text{см}}$ — установленный период смены состояний), а каждое состояние представлено ячейкой $F_j \bigcap T_i$ (рис. 1*а*).

В этом случае каждому номиналу рабочей частоты (полосе частот) соответствует вполне определенное упорядоченное (факторизованное) значение.

Другим подпространством существования полезного сигнала является сигнатурное подпространство, представляющее собой некоторую область изменяемого во времени состояния структуры и параметров сигнала [2], которые определяют содержание передаваемой команды.

В общем случае данное подпространство может быть многомерным, что в некоторой степени затрудняет его факторизацию, но для каналов управления сигнатурное подпространство может рассматриваться на уровне передаваемой кодовой комбинации, поэтому его факторизацию уместно осуществить на основе хеммингова расстояния по коду [3]. Тогда каждому состоянию можно поставить в соответствие ячейку с кодовой комбинацией в определенном временном интервале $\Delta T$, геометрически представленную полосковой структурой с $\Delta S = \text{const}$, $\Delta T = T_{\text{см}} = \text{const}$, как $S_k \bigcap T_i, k = \overline{1,K}, i = \overline{1,\infty}$ (рис. 1*б*).

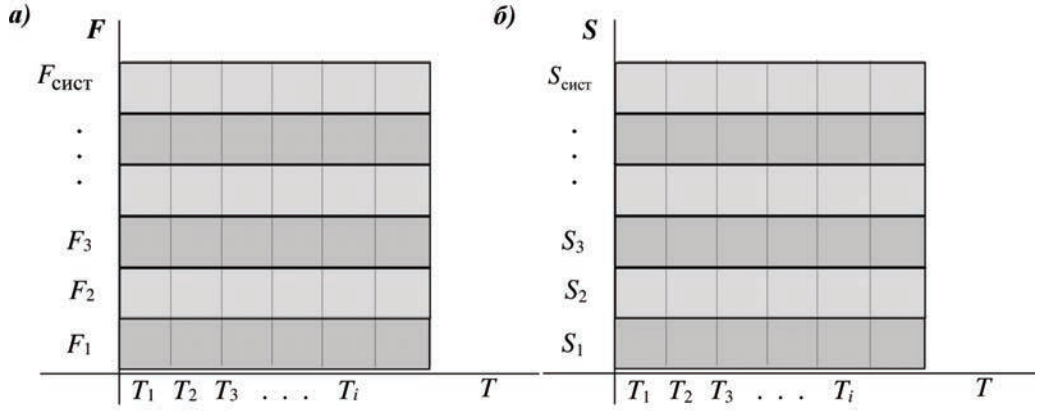



**Рис. 1.** Геометрическое представление подпространств существования сигнала: частотно-временное – *а*); сигнатурно-временное – *б*)

Поскольку частотное и сигнатурное подпространства не коррелируемы, то результирующее пространство образует ортонормированный базис, в котором каждое состояние можно представить вектором $\mathbf{R} = (F_j, S_k, T_i)$.

В полученной интерпретации пространства $\Omega_{F,S}$ каждое состояние радиоканала будет определяться некоторой ячейкой, образованной пересечением полосовой структуры с $\Delta F = \text{const}$, $\Delta S = \text{const} \rightarrow F_j \bigcap S_k$ (см. рис. 2).

В рассматриваемой структуре интервал изменения состояния определяется значением $T_{\text{см}}$. Таким образом, в итоге получаем полудискретное трехмерное пространство, в котором состояние радиоканала в пространстве $\Omega_{F,S}$ скачкообразно изменяется в масштабе времени по определенному псевдослучайному закону, независимо в каждом подпространстве $\Omega_F$ и $\Omega_S$.

В общем случае канал управления можно представить в виде вектора состояния $\mathbf{R}_m$ в пространстве $\mathbf{V}\{x_1, x_2, \ldots x_n\}$, ограниченного количеством возможных дискретных реализаций частот и числом структурных комбинаций сигнала $\mathbf{V}\{F_j \in F_{\text{сист}}, S_k \in S_{\text{сист}}\}$. В каждый момент времени в течение $T_{\text{см}}$ рабочее состояние вектора $\mathbf{R}_m$ определено областью единичного подпространства $\Omega_{\text{ед}}$, дискретно изменяемого в масштабе ограниченной области через установленные интервалы вре-

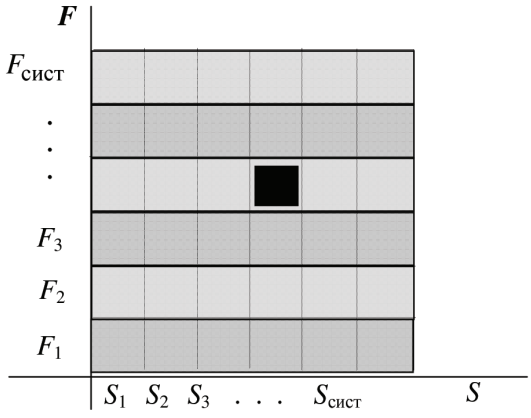



**Рис. 2.** Частотно-сигнатурное подпространство состояний радиоканала в некотором интервале времени $T_i$

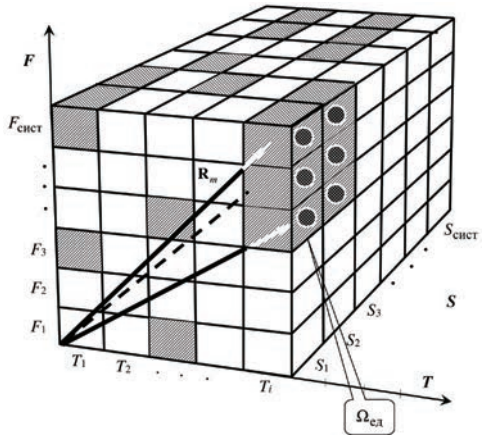



**Рис. 3.** Пространство состояний радиоканала телеметрической системы

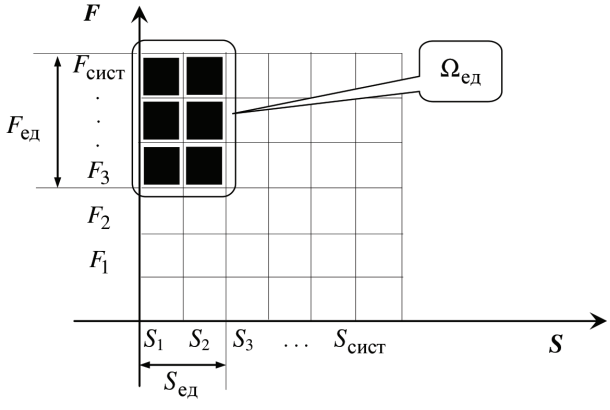



**Рис. 4.** Сечение пространства состояний системы радиосвязи в некотором интервале времени $T_i$

мени $T_{см}$ (см. рис. 3). При этом в общем случае само подпространство $\Omega_{ед}$ может быть рассредоточено во всем пространстве $\Omega_{F,S}$.

Использование сменных состояний вектора $\mathbf{R}_m$ в частотно-временном подпространстве в [2] определено как частотная имитационная защита, поэтому по аналогии, изменения в сигнатурно-частотно-временном пространстве определим как частотно-сигнатурная имитационная защита.

Определение вектора состояний в частотно-сигнатурном пространстве позволяет процесс воздействия имитационной помехи на радиоканал в режиме «Ожидание» интерпретировать как передачу ложного вектора $\mathbf{R}_{m\ лож}$ из этого же пространства. При этом уровень имитостойкости радиоканала будет определяться уровнем неопределенности, характеризуемого значением изменений состояний радиоканалов в течение времени.

С учетом рассмотренной методологии вероятность наступления того или иного состояния (вероятностная мера пространства **V**) будет определяться как

$$P(\Omega_{s4}) = P(\Omega_{F54})\, P(\Omega_{S54}), \qquad (1)$$

где $P(\Omega_{F_{ед}})$ — вероятность попадания в подобласть разрешенного состояния системы в частотном подпространстве; $P(\Omega_{S_{ед}})$ — вероятность попадания в подобласть разрешенного состояния системы в сигнатурном подпространстве.

По аналогии с системами криптографической защиты [4], наибольший уровень неопределенности возникает в том случае, если изменение состояний канала происходит по равномерному закону. В этом случае обеспечивается максимальная имитозащищенность. В таких условиях вероятность имитонавязывания за одну попытку в пределах определенного сечения пространства, т.е. за время $T_{см}$ (см. рис. 4) определяется отношением числа состояний в единичном подпространстве $\Omega_{ед}$ к общему числу возможных состояний в сечении подпространства $\Omega_{сист}$, которое с учетом независимости состояний в частотном и сигнатурном подпространствах радиоканала определяется выражением:

$$p_1 = \frac{\Omega_{ед}}{\Omega_{сист}} = \frac{F_{ед} S_{ед}}{F_{сист} S_{сист}}, \qquad (2)$$

где $S_{ед}$ — число комбинаций сигнатуры системы, соответствующее единичному состоянию радиоканала $|_{S54}$; $F_{ед}$ – число состояний вектора в частотном подпространстве $|_{F54}$, соответствующее единичному состоянию радиоканала; $S_{сист}$ – число возможных комбинаций сигнатуры системы; $F_{сист}$ – число возможных реализаций вектора в частотном пространстве (диапазон рабочих частот).

Согласно полученному выражению (2), чем больше число возможных состояний канала, тем ниже вероятность имитанавязывания и, соответственно, выше его имитостойкость.

Однако такая оценка не всегда отражает реальную эффективность имитационной воздействия, так как существует возможность прямого перебора всех возможных состояний, в результате которого в некоторых случаях при достаточно малых значениях $p_1$ реальная возможность имитации будет достаточно высокой. Для анализа последствий имитонавязывания предлагается следующая модель, учитывающая особенности радиоканала управления в режиме «Ожидание» и воздействующую на него имитационные помехи (см. рис. 5).

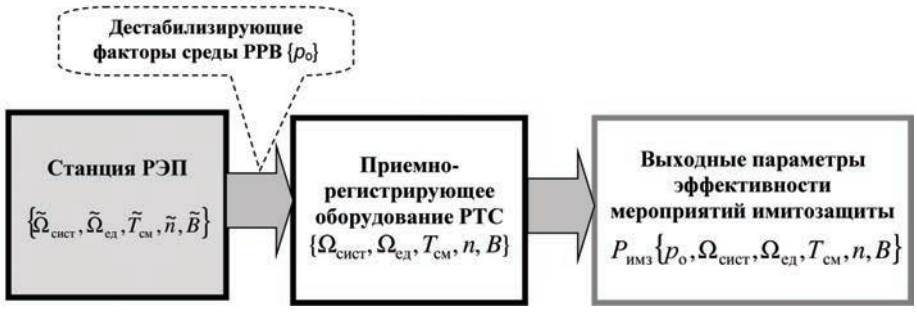



**Рис. 5.** Модель воздействия имитационных помех на радиоканалы управления БПЛА

В модели, эффективность мероприятий имитозащиты определяется вероятностью $p_{имз}$, в которой, кроме множества состояний, учитывается время их смены ($T_{см}$), параметры радиоканала ($n$ — длина синхропосылки, $B$ — скорость манипуляции) и дестабилизирующие факторы среды распространения радиоволн ($p_o$ — вероятность ошибки приема бита информации).

Особенность каналов управления БПЛА состоит в ограниченности используемого в них частотно-сигнатурного ресурса, что связано с характером распространения радиоволн, конечностью алфавита подаваемых допустимым временным интервалом передачи команды и т. д. Это позволяет с достаточно высокой точностью $\tilde{\Omega}_{F,S} \to \Omega_{F,S}$ получить оценку границ всего частотно-сигнатурного пространства в интересах применения сравнительно простых процедур поиска требуемого состояния, основанных на сканировании частотно-сигнатурного пространства $\Omega_{F,S}$.

Поскольку процесс имитационного воздействия представляет собою последовательное многоразовое сканирование пространства состояний $\Omega_{F,S}$, представленного простейшим потоком Бернулли, то при известных параметрах $\{\tilde{\Omega}_{сист}, \tilde{\Omega}_{ед}, \tilde{T}_{см}, \tilde{n}, \tilde{B}\} \to \{\Omega_{сист}, \Omega_{ед}, T_{см}, n, B\}$ среди бернуллиевых схем оптимальной является метод на основе гипергеометрической логике сканирования [5].

Оценка эффективности такого сканирования определяется известным выражением гипергеометрического распределения:

$$H\left(\xi;\ K, \Omega_{ед}, \Omega_{сист}\right) = \binom{\Omega_{ед}}{\xi}\binom{\Omega_{сист} - \Omega_{ед}}{K - \xi}\Big/\binom{\Omega_{сист}}{K}, \tag{3}$$

с временем гарантированного выбора разрешенного состояния:

$$T_{гар} = \frac{n}{B}\left(\Omega_{сист} - \Omega_{ед} + 1\right), \tag{4}$$

где $\Omega_{ед} = F_{ед}S_{ед}$ (в рассматриваемом случае $S_{ед}$ — число комбинаций сигнатуры системы, соответствующее единичному состоянию радиоканала; $F_{ед}$ — число состояний вектора в частотном подпространстве, соответствующее единичному состоянию радиоканала), $\Omega_{сист} = F_{сист}S_{сист}$ ($S_{сист}$ — число возможных комбинаций сигнатуры системы; $F_{сист}$ — число возможных реализаций вектора в частотном пространстве (диапазон рабочих частот)), $K = \mathrm{Int}[BT_{ИП}/n]$ — целое число попыток сканирования, определяемое временем воздействия имитационной помехой $T_{ИП} < T_{гар}$, скоростью манипуляции $B$ и длиной синхропосылки сигнала $n$, $\xi$ — необходимое число попаданий на разрешенные состояния за время имитационного воздействия, требуемое для эффективного имитонавязывания тем или иным способом.

Таким образом, формула (3) является универсальной оценкой эффективности воздействия имитационной помехи для модели на рис. 6.

Выражение (3) позволяет определить критериальное решающее правило ($\Omega_{сист} = F_{сист}S_{сист}$; $\Omega_{ед} = F_{ед}S_{ед}$), задавшись параметрами гипергеометрической статистики.

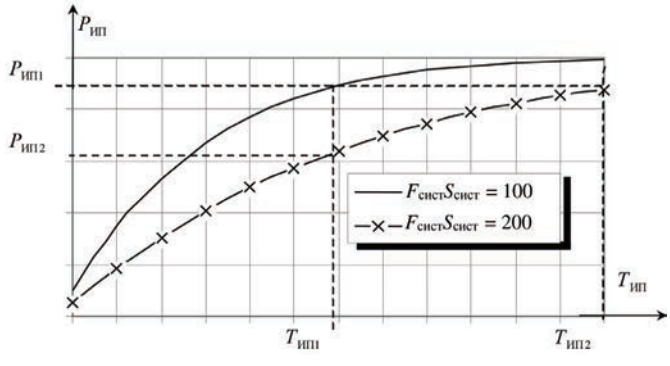



**Рис. 5.** Модель воздействия имитационных помех на радиоканалы управления БПЛА

**Заключение**

Поскольку результирующая оценка $H(*)$ носит вероятностный характер, то достижение конкретного заданного значения $H_з(*)$, можно интерпретировать как вероятность обеспечения мероприятий по имитозащите радиоканала $p_{ИП}$, что в свою очередь позволяет для рассматриваемых условий и параметров связать ее значение (вероятности) со временем, необходимым для ее получения.

Другими словами, если задаться некоторым вероятностным уровнем $p_{ИП1}$ (см. рис. 6), то можно оценить время его достижения $T_{ИП1}$, и наоборот, задавшись временными ограничениями $T_{ИП1}$ и $T_{ИП2}$, можно по конкретным зависимостям определить соответствующее вероятностное значение $p_{ИП1}$ и $p_{ИП2}$.

**Список литературы**

1. Орощук И. М., Аксенов В. П. Технологические особенности применения десинхронизирующих имитопомех в автоматизированных системах связи // Международная конференция по телекоммуникациям (IEEE/ICC2001/ St. Petersburg), Санкт-Петербург, 2001. С. 4–8.

2. Вознюк В. В., Крячко А. Ф., Попов Е. А. Принципы радиоэлектронного противодействия в системах передачи информации. СПб.: Изд-во Политехн. Ун-та, 2008. 246 с.

3. Голяницкий И. А. Математические модели и методы в радиосвязи / Под ред. Ю. А. Громакова. М.: Эко-трендз, 2005. 440 с.

4. Нечаев В. И. Элементы криптографии (Основы теории защиты информации) / Под ред. В. А. Садовничего. М.: Высшая школа, 1999. 109 с.

5. Куприянов А. И., Сахаров А. В. Радиоэлектронные системы в информационном конфликте. М.: Вузовская книга, 2007. 528 с.

## PROPOSALS FOR EXPOSURE DEVELOPMENT OF MATHEMATICAL MODELS SIMULATION INTERFERENCE ON THE CONTROL CHANNEL OF THE UAV IN THE «STANDBY»

**Ivanov Roman Vyacheslavovich,**
St. Petersburg, Russia, demon13_84@mail.ru

**Abstract**

It is proved that the technical development of systems cybernetics largely changed the face of warfare and led to the widespread use of drones, which play a significant role on the battlefield, so the issues anti-jamming their control channels NElyayutsya relevant and meaningful for both developers and professionals engaged in the operation of vehicles.

It is shown that the most dangerous structural noise due to the difficulties of identifying them.

These circumstances determine the relevance of the development of simulation models of the impact of noise on the control channels of unmanned aerial-enforcement units in the "Waiting", which will develop measures to combat the imposition of false commands and impaired functioning of the receiving equipment.

This paper analyzes the features of the regime "Waiting" from the standpoint of the possible states of the apparatus. Described geometric space sous-existence of available signals. It substantiated its multidimensionality, and separately-allocated by the signature component of the vector signal states as their defining characteristic. Presented and described frequency signature-temporary state control channel (telemetry) from the position of the area of its allowable values. Subject to consideration the methodology defined-DELENA probability of occurrence of a state of the channel as the Vero-surface area measures its allowable values.

It is shown that, by analogy with the systems of cryptographic protection, NAI-greater level of uncertainty arises when changing channel conditions occurs on uniform law, as in this case of SLE, a simulation provides maximum security. Only in these conditions, the probability of simulation for imposing one attempt within a predetermined time is determined by the ratio of the number of states in the subspace unit to the total number of possible states.

To analyze the consequences of the proposed imposition of simulation mo-del, taking into account the peculiarities of radio control in the "Waiting", taking into account all the analyzed factors.

**Keywords:** mathematical model of the impact of interference imitatsitatsionnyh; UAV control channel; geometric space signals.

**References**

1. Oroschuk IM, Aksenov V.P Technological features desynchronizing imitopomeh use in automated communications systems. International Conference on Telecommunications (IEEE / ICC2001 / St. Petersburg), St. Petersburg, 2001. Pp. 4–8.

2. Voznyuk V. V., Kryachko A. F., Popov E. A., Principles of electronic countermeasures in communication systems. St. Petersburg, Publishing House of the Polytechnic University, 2008. 246 p.

3. Golyanitsky I. A., YA Gromakova Y. A. (Ed.). Mathematical models and methods in radio. Moscow, Eco-Trendz, 2005. 440 p.

4. Nechayev V. I., Sadovnichy V. A. (Ed.). Elements of cryptography (foundations of the theory of information security): Textbook for universities and colleges. Moscow, Higher School, 1999. 109 p.

5. Kupriyanov A. I., Zakharov A. V., Electronic systems in the information conflict. Moscow, High school book, 2007. 528 p.

**Information about author:**
Ivanov R. V., laboratory of the department, Military Communications Academy

# РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ СОВРЕМЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УЧЕТА МЕДИЦИНСКОГО ИМУЩЕСТВА В ВОЕННОЕ ВРЕМЯ

**Мирошниченко Юрий Владимирович,**
д.фарм.н., профессор, заслуженный работник здравоохранения, заведующий кафедры Военно-медицинской академии имени С.М. Кирова, Санкт-Петербург, Россия, miryv61@mail.ru

**Кононов Владимир Николаевич,**
к.фарм.н., заместитель начальника кафедры Военно-медицинской академии имени С.М. Кирова, Санкт-Петербург, Россия

**Родионов Евгений Олегович,**
к.фарм.н., преподаватель Военно-медицинская академия имени С.М. Кирова, Санкт-Петербург, Россия

**Аннотация**
Раскрыты недостатки традиционных способов ведения учета медицинского имущества в медицинских подразделениях соединений и воинских частей в военное время. Показана актуальность создания автоматизированной системы учета медицинского имущества в военное время с применением средств электронной вычислительной техники, а также установлены требования, предъявляемые к ее работе в особых условиях. Представлена характеристика современного программно-аппаратного комплекса для учета медицинского имущества в войсковом звене медицинской службы, включенного в состав принятого на снабжение Вооруженных Сил Российской Федерации комплекта медицинского имущества «Бланки и книги медицинского учета и отчетности (войсковой)». Показан алгоритм разработки и порядок работы специализированного программного обеспечения для учета медицинского имущества в медицинских подразделениях соединений и воинских частей в военное время.

**Ключевые слова:** *войсковое звено медицинской службы, медицинское имущество, программно-аппаратный комплекс, специализированное программное обеспечение, учет.*

Учет *медицинского имущества* (МИ) относится к важнейшим направлениям деятельности системы медицинского снабжения войск (сил). Во многом это связано с тем, что наличие достоверной ученой информации является ключевым условием для правильного определения потребности, истребования, распределения и отпуска МИ, а также способствует принятию обоснованных управленческих решений при организации медицинского обеспечения соединений и воинских частей Вооруженных Сил Российской Федерации (ВС РФ). Учет МИ должен быть своевременным, полным, достоверным и точным, вестись в любых условиях обстановки и не зависеть от характера деятельности медицинских подразделений (организаций) [3, 5]. Эффективное выполнение этих требований возможно только путем использования современных *программно-аппаратных комплексов* (ПАК).

Анализ опыта обеспечения МИ войск (сил) в различных вооруженных конфликтах и чрезвычайных ситуациях свидетельствует, что традиционно используемые для ведения учета технологии, технические средства и носители информации имеют ряд недостатков, к основным из которых относятся [1, 2]:

значительная трудоемкость процедур отработки учетных и отчетно-заявочных документов, а также их аналитической и статистической обработки;

высокая вероятность повреждения (утраты, несанкционированного доступа и т.д.) технических средств и носителей информации;

существенные затраты времени на передачу в вышестоящий орган (звено) медицинской службы соответствующей информации и низкая надежность этого процесса.

Вместе с тем, современный уровень развития компьютерных и информационно-коммуникационных технологий, а также новые требования к управлению ресурсами МИ предопределяют необходимость использования защищенных средств электронной вычислительной техники и *специализированного программного обеспечения* (СПО) для обработки учетных данных и составления отчетно-заявочных документов. Исходя из этого специалистами *Военно-медицинской академии им. С.М. Кирова* (ВМА) совместно с ООО «Специальная и Медицинская техника» и ООО «Лаборатория синтеза систем безопасности» был разработан ПАК для ведения учета МИ в войсковом звене медицинской службы, состоящий из *переносного защищенного персонального компьютера* (ПЗПК) с печатающим устройством и СПО «Учет МИ воинской части (соединения)».

ПАК включен в состав комплекта МИ «Бланки и книги медицинского учета и отчетности (войсковой)» (шифр – КБК), принятого на снабжение ВС РФ и включенного в нормы снабжения МИ соединений, воинских частей и организаций ВС РФ на военное время[1]. Опись указанного комплекта утверждена начальником Главного военно-медицинского управления Министерства обороны РФ**.

***Характеристика средств электронной вычислительной техники.*** ПЗПК и печатающее устройство (принтер), входящие в состав ПАК, обладают ударопрочными, износостойкими и защищенными от воздействия неблагоприятных факторов внешней среды (пыле- и влаго-непроницаемость, герметичность и др.). Элементная база ПЗПК позволяет оперативно обрабатывать большие объемы информации (таблицы, графики и др.). Исходя из требований по защите обрабатываемой информации, на него необходимо устанавливать отечественную инновационную *операционную систему специального назначения* (ОССН) «Astra Linux Special Edition» (система сертифицирована во всех трех системах сертификации средств защиты информации — Министерство обороны РФ, Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности РФ).

Помимо этого, к ПАК предъявляются дополнительные требования, обусловленные его работой в особых условиях. В этой связи, все его компоненты должны функционировать при температуре окружающей среды от –21 °С до +60 °С, относительной влажности воздуха до 95% и др. Кроме того, ПАК должен обеспечивать автономную работу специалистов на протяжении длительного времени.

***Алгоритм разработки СПО «Учет МИ воинской части (соединения)».*** Требования к электронной вычислительной технике и ОССН предопределили особенности разработки и последующей эксплуатации СПО для учета МИ в войсковом звене медицинской службы в военное время, которое должно обеспечивать автоматизацию учетных операций по движению различных видов МИ (лекарственные средства, медицинские изделия расходные и инвентарные и др.), определения потребности в МИ, формирование отчетно-заявочных документов (донесение о наличии и потребности МИ специального назначения, заявка-наряд на МИ и материалы для ремонта и др.) и т.д.

Разработка СПО проводилась в несколько этапов. На первом этапе был проанализирован порядок оформления учетных документов, определены содержание и объем задач по учету МИ в военное время. Это позволило определить характер обрабатываемых данных, а также структуру и содержание *баз данных* (БД). Второй этап включал создание механизмов функционирования и взаимодействия БД, а также выработку алгоритма работы всего СПО (например, отработку формул и порядка расчета потребности в МИ). Этап отладки и апробации предусматривал проведение натурных испытаний (проводились на базе ВМА в ходе тактико-специальных учений). Анализ полученных результатов позволил выявить некоторые недостатки, обусловленные особенностями ведения учета МИ в режиме реального времени (определение потребности, дефектуры и др.). Далее проводилась адаптация СПО к ОССН, устранение выявленных недостатков, а также внедрение ПАК в деятельность медицинских подразделений (организаций) и обучение специалистов работе с ним (для методического сопровождения СПО была разработана инструкция по эксплуатации). На завершающем этапе выполнялись установленные процедуры по государственной регистрации СПО, в результате которых было получено Свидетельство о государственной регистрации программы для ЭВМ от 20 мая 2015 г. № 2015615513 «СПО: Учет МИ воинской части (соединения) (СПО-МС-У)».

Алгоритм разработки СПО «Учет МИ воинской части (соединения)», представлен на рис. 1.

***Порядок работы со СПО «Учет МИ воинской части (соединения)».*** Алгоритм работы СПО основывается на четырех блоках распределения информации и схематично представлен на рис. 2.

При подготовке СПО к работе производится обобщение исходных и текущих данных, которые, в свою очередь, сопоставляются со справочной информацией и соответствующими БД. К исходным данным относится информация об обеспечиваемом подразделении (численность личного состава и медицинского персонала, количество коек и др.), а также данные о наличии МИ к началу работы. Эти данные вводятся единовременно, а их наличие является обязательным

[1]Приказы Министра обороны РФ от 21.05.2011 г. № 744 «О принятии на снабжение Вооруженных Сил Российской Федерации изделий комплектно-табельного оснащения медицинской службы Вооруженных Сил Российской Федерации», от 18.03.2015 г. № 147 «Об утверждении Норм снабжения медицинским имуществом медицинских и фармацевтических организаций (подразделений) Вооруженных Сил Российской Федерации на военное время», от 18.12.2012 г. № 3740 «Об утверждении Норм снабжения медицинским имуществом соединений, воинских частей и организаций Вооруженных Сил Российской Федерации и запасов на военное время»

**Приказ начальника Главного военно-медицинского управления Министерства обороны Российской Федерации от 12.07.2011 г. № 77 «Об утверждении Сборника описей комплектов медицинского имущества для войскового звена медицинской службы Вооруженных Сил Российской Федерации на военное время» (в редакции с изменениями, утвержденными приказ начальника Главного военно-медицинского управления Министерства обороны Российской Федерации от 25.03.2015 г. № 26).


**Рис. 1.** Алгоритм разработки СПО «Учет МИ воинской части (соединения)»

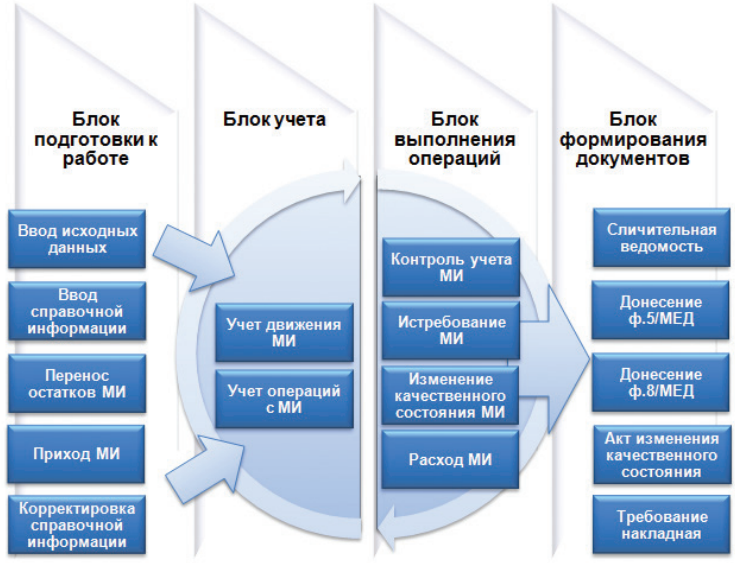



**Рис. 2.** Схема работы СПО по учету МИ в военное время

для дальнейшего функционирования СПО. К текущим данным относятся учетные данные о движении МИ в ходе дальнейшей работы. Справочная информация интегрирована в СПО и содержит данные нормативных правовых актов и служебных документов Министерства обороны РФ (нормы снабжения МИ, описи комплектов МИ, перечни МИ военного и специального назначения и др.). Для актуализации справочной информации предусмотрена возможность их корректировки.

Результатом подготовки СПО к работе является формирование единой БД обеспечиваемого подразделения, которая в дальнейшем служит основой для ведения учета МИ. На этой стадии СПО считается полностью готовым к проведению учетных операций (изменение качественного состояния, отпуск, определение потребности, составление отчетно-заявочных документов и др.).

Данные о проведении приходных операций вводятся на основании первичных учетных (вспомогательных) документов (наряд, накладная, акт и др.). Полученное МИ может быть поставлено на учет как покомплектно, так и по разрозненной номенклатуре. Для упрощения процесса ввода информации предусмотрен выбор номенклатурных позиций МИ из БД.


**Рис. 3.** Распределение потоков информации при работе ПАК

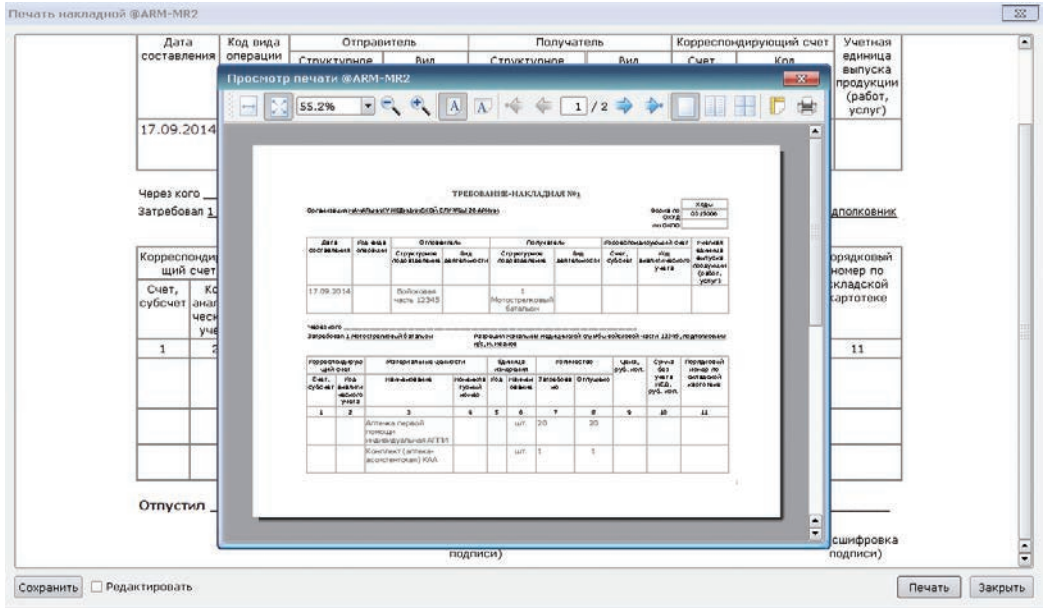



**Рис. 4.** Внешний вид оформления операции по отпуску МИ

Порядок использования данных при выполнении учетных операций представлен на рис. 3.

При оформлении расхода МИ формируется требование-накладная, в которой заголовочная и оформляющая части заполняется автоматически, а содержательная — основываясь на данных о выбранных к отпуску (выдаче) образцах МИ (рис. 4). Кроме того, в СПО предусматривается регистрация расходных документов.

При составлении отчетно-заявочных документов их заголовочные и оформляющие части заполняется автоматически. Также на основании исходных и справочных данных автоматически рассчитывается штатно-табельная (табельная) потребность в МИ. Помимо заголовочной и оформляющей частей автоматически формируются и некоторые данные в содержательной части (наличие, приход и расход МИ за отчетный период и др.). Для заполнения данных о фактической потребности предусматривается возможность редактирования содержательной части и составления пояснительной записки.

Контрольная функция СПО реализуется путем обобщения информации о наличии МИ в подразделении. Сформированная для этих целей сличительная ведомость выводится на печать и может использоваться для проведения инвентаризации МИ.

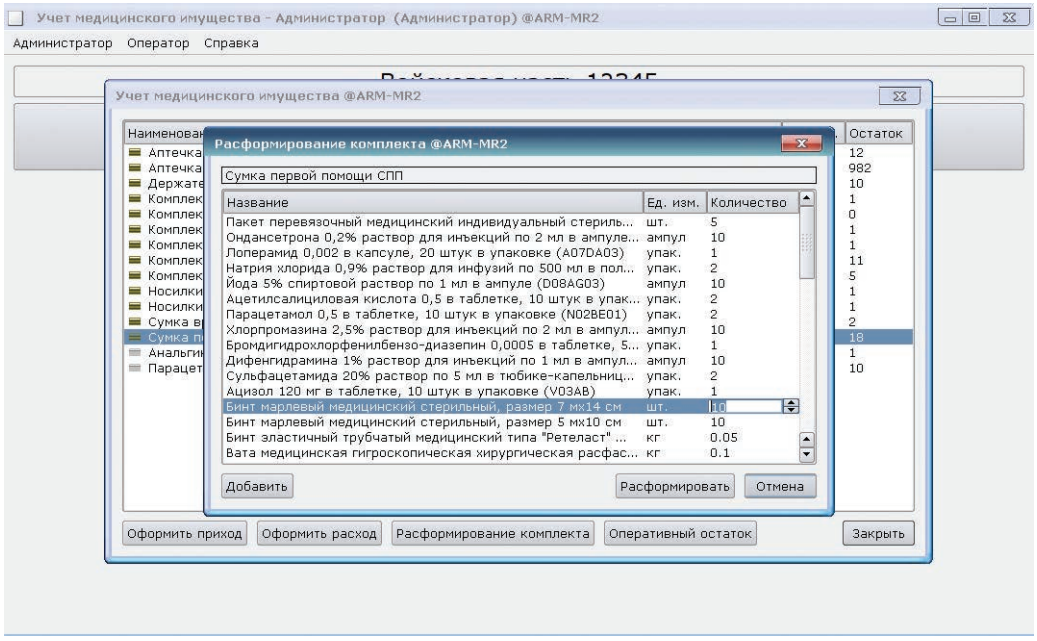



**Рис. 5.** Внешний вид операции по расформированию комплектов МИ

В СПО автоматизирована важная операция документального оформления процедуры расформирования комплектов МИ. Справочные данные, содержащие информацию о номенклатуре и количестве МИ в комплектах, способствуют ускорению оформления операции, позволяя пользователю подтверждать или изменять необходимую информацию (рис. 5).

В настоящее время в рамках выполнения государственного оборонного заказа осуществляется поставка в войска современных образцов комплектно-табельного оснащения, в том числе и комплектов КБК и БК-2. Кроме того, ПАК для учета МИ в войсковом звене медицинской службы используется в учебном процессе ВМА, обеспечивая возможность обучения курсантов и слушателей передовым технологиям учета МИ в военное время.

Таким образом, современный ПАК для учета МИ в войсковом звене медицинской службы позволяет в любых условиях обстановки эффективно решать ряд важных задач по учету МИ, что в свою очередь способствует своевременному и бесперебойному обеспечению им соединений и воинских частей.

**Список литературы**

1. Кононов В. Н., Мирошниченко Ю. В., Тихонов А. В., Родионов Е. О. Современные подходы к ведению учета медицинского имущества в войсковом звене медицинской службы // Никифоровские чтения — 2015: Передовые отечественные и зарубежные медицинские технологии: Сб. материалов научно-практической конференции молодых ученых и специалистов, Санкт-Петербург, Всероссийский центр экстренной и радиационной медицины им. А. М. Никифорова МЧС России, 11–12 сентября 2015 г. СПб.: Политехника-принт, 2015. 66 с.

2. Мирошниченко Ю. В., Горячев А. Б., Беня Ф. М. Опыт медицинского снабжения войск в вооруженном конфликте на территории Южной Осетии // Воен.-мед. журн. 2009. № 1. С. 68–72.

3. Мирошниченко Ю. В., Бунин С. А., Кононов В. Н. Организация обеспечения медицинским имуществом воинской части. СПб.: ООО СРП «Павел» ВОГ, 2014. 200 с.

4. Мирошниченко Ю. В., Бунин С. А., Горячев А. Б., Иванов В. В., Моргунов В. А., Голубенко Р. А., Гайнов В. С., Тихонов А. В. Концептуальные подходы к автоматизации управления ресурсами медицинского имущества // Вестник Российской Воен.-мед. акад. 2012. № 1 (37). С. 251–255.

5. Мирошниченко, Ю.В., Горячев А. Б., Бунин С. А., Умаров С. З., Косолапов В. Н. Учет медицинского имущества; под общей редакцией проф. Ю. В. Мирошниченко. СПб.: ВМА, 2009. 120 с.

## DEVELOPMENT AND USE OF THE MODERN AUTOMATED SYSTEM OF THE ACCOUNTING OF MEDICAL PROPERTY IN THE WARTIME

**Miroshnichenko Yurii Vladimirovich,**
St.Peterburg, Russia, miryv61@mail.ru

**Cononov Vladimir Nikolaevich,**
St.Peterburg, Russia

**Rodionov Evgenii Olegovich,**
St.Peterburg, Russia

**Abstract**
Shortcomings of traditional ways of maintaining the accounting of medical property of medical divisions of connections and military units in wartime are opened. The urgency of creation of the automated system of the accounting of medical property in wartime with application of means of electronic computer facilities is shown, and also the requirements shown to its work in special conditions are established. The characteristic of a modern hardware-software complex for the accounting of medical property in an army link of the health service, included in structure accepted on supply of Armed forces of the Russian Federation of a set of medical property «Forms and books of the medical account and the reporting (army)» is presented. The algorithm of development and an operating procedure of the specialized software for the accounting of medical property in medical divisions of connections and military units in wartime are shown.

**Keywords:** army link of a health service, medical property, hardware-software complex, specialized software, account.

**References**
1. Kononov V.N., Miroshnichenko Yu.V., Tikhonov A.V., Rodionov E.O. Modern approaches to maintaining the accounting of medical property in an army link health service. Nikiforovsky chteniya 2015: Advanced domestic and foreign medical technologies: Digest materials of scientific and practical conference of young scientists and experts, St. Petersburg, the All-Russia center of emergency and radiating medicine of A.M.Nikiforova of the Ministry of Emergency Situations of Russia, on September 11-12, 2015 SPb.: Politehnica-print, 2015. P. 66.
2. Miroshnichenko Yu.V., Goryachev A.B., Benya F.M. Experience of medical supply of armies in armed conflict in the territory of South Ossetia .Voyen. - medical magazine. 2009. No. 1. Pp 68-72.
3. Miroshnichenko Yu.V., Bunin S. A., V.N. Organization of providing with medical property of military unit. SPb.: SRP "Pavel" of VOG, 2014. P. 200.
4. Miroshnichenko Yu.V., Bunin S.A., Goryachev A.B., Ivanov V.V., Morgunov V.A., Golubenko R.A., Gaynov V. S., Tikhonov A.V. Conceptual approaches to automation of resource management of medical property. Russian Voyen's - medical academy. 2012. No. 1 (37). Pp 251-255.
5. Miroshnichenko Yu.V., Goryachev A.B., Bunin S. A., Umarov S. Z., Kosolapov V. N. Accounting of medical property; under the general edition of prof. Yu.V.Miroshnichenko. SPb.: VMA, 2009. 120 p.

**Information about author:**
Miroshnichenko Yu.V., Ph.D., Military medical academy of a name of Page of S.M. Kirov
Cononov V.N., Ph.D., Military medical academy of a name of Page of S.M. Kirov
Rodionov E.O., Ph.D., Military medical academy of a name of Page of S.M. Kirov

# СОВРЕМЕННЫЕ ТЕХНОЛОГИИ СТАТИЧЕСКОГО И ДИНАМИЧЕСКОГО АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**Чукляев Евгений Игоревич,**
*научный сотрудник Смоленской общественной организации содействия науки и образованию «Региональный союз ученых» г. Смоленск, Россия, smolrsu@mail.ru*

**Аннотация**
В статье представлены результаты анализа существующих подходов защиты и идентификации дефектов (уязвимостей и ошибок) в исходном и бинарном кодах программ, проводимых на различных этапах их разработки, проектирования и эксплуатации. Обобщены наиболее распространенные дефекты кода и объекты воздействия, функциональные и эргономические требования, предъявляемые к современным системам анализа.

**Ключевые слова:** статический и динамический анализ; исходный и бинарный код; дефекты (уязвимости и ошибки); требования, технологии защиты; объекты несанкционированных воздействий.

Поиск и устранение дефектов в программном обеспечении (ПО) требует больших трудозатрат, при этом многие из них могут остаться незамеченными. По данным исследования, проведенного по заказу Национального института стандартов и технологий США, убытки, возникающие из-за недостаточно развитой инфраструктуры устранения дефектов в ПО (уязвимостей и некритических ошибок), составляют от 22 до 60 миллиардов долларов в год [8], часто являются причиной переноса сроков выпуска программ. Стоимость устранения дефекта, пропущенного на этапах разработки и тестирования, может возрасти после поставки программы от 2 до 100 раз [9].

Как следствие, наибольшее распространение получили методы *статического анализа* исходного кода ПО, рассматривающие все возможные пути выполнения программы без ее фактического выполнения. Дело в том, что такие методы реализуются в системах, полностью интегрируемые в цикл разработки ПО, применяемые как на этапе тестирования, так и на более ранних этапах — в ходе разработки, причем как во время, так называемых, «ночных сборок», так и непосредственно на аппаратуре разработчика.

Применение систем поиска дефектов (уязвимостей и некритических ошибок) ПО в промышленном масштабе обуславливает следующие *функциональные и эргономические требования*:

минимальные действия пользователя для интеграции инструмента анализа в систему сборки ПО (отсутствие необходимости в изменении, аннотировании, интегрировании в процесс анализа исходного кода ПО);

автоматический поиск дефектов и уязвимостей (без участия пользователя непосредственно в процессе анализа);

масштабируемость анализа (проведение анализа объемом нескольких миллионов строк кода и сотен тысяч функций);

низкий процент ложных срабатываний (значительная часть выдаваемых предупреждений должна быть истинной; приемлемым считается уровень в 30–50% истинных срабатываний, а для важнейших — около 70%);

расширяемость инфраструктуры анализа (дополнение алгоритмами идентификации различными новыми классами уязвимостей (дефектов и критических ошибок);

удобный пользовательский интерфейс просмотра результатов и настройки инструмента анализа.

В свою очередь, описанные требования влекут необходимость реализации следующих технологий системы анализа:

анализ без доступа к полному исходному коду анализируемого ПО (наличие в инструменте анализа внутренних спецификаций, позволяющих описывать действия стандартных библиотечных функций объекта анализа);

выполнение глубокого межпроцедурного анализа (возможность учета влияния разных функций на поведение ПО при поиске заданных ситуаций);

инкрементальный анализ (т.е. анализ только измененной части проекта при наличии полных результатов анализа старой версии проекта);

проведение удаленного анализа, поддержка нескольких разработчиков, ведение истории результатов анализа.

Необходимо отметить, что даже при выполнении всех упомянутых требований методы статического анализа имеют ряд ограничений, не позволяющих в ряде случаев достигнуть высокой точности анализа. Во-первых, при отсутствии полного исходного кода программы возникает неопределенность, не связанная непосредственно с качеством анализа: в зависимости от свойств недоступного при анализе кода, некоторая операция может как приводить, так и не приводить

к ошибке. Например, для библиотечного кода часто возможно построение некорректного вызова из пользовательского кода, приводящего к выполнению некорректной операции в коде библиотеки, но при отсутствии кода этого вызова ошибка в коде библиотеки, как правило, диагностироваться не должна.

Во-вторых, независимо точности статического анализа при обнаружении конструкций, которые могут потенциально указывать на уязвимость, во многих случаях не удается установить, возможен ли в действительности путь исполнения программы и входные данные, приводящие к ошибке. Выдача всех предупреждений в таких ситуациях приводит к тому, что большая их доля оказывается ложной, делая систему статического анализа малополезной для многих приложений.

Наконец, для больших программных систем (в миллионы строк кода) не удается за приемлемое время провести точный межпроцедурный анализ даже имеющегося кода, с учетом необходимости выполнять анализ указателей, интервальный анализ (анализ возможных значений переменных).

Как следствие упомянутых ограничений, промышленные коммерческие анализаторы вынуждены использовать эвристические алгоритмы анализа: при отборе важнейших (с точки зрения анализа) данных о программе среди полученных, при поиске конкретных ситуаций (шаблонов) в потоке данных и управления программы; и последующей выдаче лишь по этим отобранным данным или ситуациям предупреждений о возможных дефектах. Иначе проценты ложных срабатываний инструмента или потребляемые им ресурсы становятся неприемлемо большими. Улучшение алгоритмов анализа или использование других видов анализа, требующих больших вычислительных ресурсов (например, символьного исполнения в комбинации с решателями логических уравнений для отсеивания ложных путей выполнения), повышает точность анализа, но в силу затрачиваемых ресурсов может применяться только к самым важным предупреждениям и сравнительно небольшим частям программы (тысячи строк кода).

Поэтому, в промышленных инструментах анализа возникают ситуации пропуска истинных дефектов как следствие ошибок эвристик, то есть выполняется *нестрогий анализ*. Разные инструменты анализа всегда выдают частично пересекающиеся множества предупреждений для одной и той же программы: часть предупреждений общая, часть — уникальна для каждого инструмента, что обусловлено различием применяемых эвристик.

Всеми заявленными свойствами из коммерческих систем, по всей видимости, обладают системы Coverity Insight [10], Klocwork K9 [11], GrammaTech CodeSonar [12], Svace ИСП РАН [13–15]. Точное суждение об архитектуре и алгоритмах анализа, положенных в основу этих систем, затруднено из-за их закрытости, равно как и сравнение результатов их работы. Проводившиеся в ИСП РАН оценки инструмента Svace на доступном для анализа материале показали качество анализа, сравнимое с остальными коммерческими системами [15].

Существуют и другие классы систем обнаружения дефектов в исходном коде программ, однако точность и требуемые для использования ресурсы ограничивают их область применения (рисунок 1). Данные системы не получили такого распространения, как упомянутые системы автоматического поиска дефектов на основе статического анализа. Из этих классов систем можно упомянуть следующие системы:

автоматизации экспертного аудита;

верификации ограниченного исходного кода;

проверки корректности пользовательских аннотаций.

Необходимо отметить, что эффективность систем автоматического поиска дефектов ПО зависит от того, на каком наборе тестовых программ нарабатывались эвристики этих систем. По умолчанию эвристики поиска ситуаций в исходном коде, ранжирования собранных данных по важности, параметры точности применяемых алгоритмов настроены на некоторое «среднее» значение поведения анализируемых программ. Так, если программист перед использованием некоторого указателя проверяет его значение на корректность во всех точках программы, кроме одной-двух, то велика вероятность, что и в этих точках программы значение указателя может быть некорректным, и требуется выдать предупреждение о возможном разыменовании нулевого указателя. Конечно, такая эвристика применяется лишь в том случае, если основные алгоритмы статического анализа не смогли с достаточной точностью установить значение указателя.

Следовательно, для специальных классов программ является возможной такая *доработка системы автоматического поиска*, что точность выполняемого системой анализа для этих классов программ повысится. При этом основные виды анализов, выполняемые системой, останутся неизменными.

Перечислим основные способы такой доработки систем автоматического поиска:

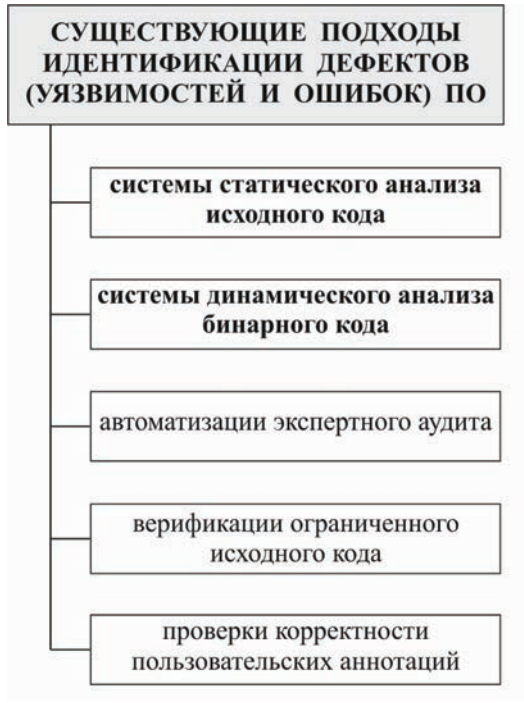



**Рис. 1.** Классы систем обнаружения дефектов в исходном коде программ

определение специфичных для данного класса программ ситуаций, сигнализирующих о дефектах в исходном коде, доработка эвристик системы для выдачи предупреждений о таких ситуациях;

настройка параметров анализа системы или применение дополнительных высокоточных методов анализа (например, чувствительных к путям выполнения) для ключевых, ограниченных по объему участков программы;

ранжирование вычисленной в ходе анализа информации по важности для конкретного класса программы (например, более точное вычисление информации о параметрах вызовов интерфейсов межпроцессного взаимодействия ОС для параллельных программ);

создание спецификаций для используемых программой библиотек, исходный код которых недоступен (как правило, система анализа знает о поведении лишь стандартных библиотек POSIX, C, C++).

Важным специальным классом программы являются системные программы, в частности, ядро и драйверы операционной системы. Как показано выше, объектами воздействия при эксплуатации уязвимостей являются чаще всего именно системные ресурсы, ошибки в привилегированных программах ОС сразу при эксплуатации позволяют добиться необходимой эскалации прав, а также дальнейшего нарушения защищенности информации. Например, при анализе ядра Linux можно создать спецификации для функций выделения и освобождения памяти, используемых в ядре, а также учесть соглашения ядра о возврате кодов ошибок из интерфейсных функций. Для встраиваемых систем, ОС реального времени можно воспользоваться относительно небольшим объемом анализируемого исходного кода и повысить точность алгоритмов анализа. Разработка и реализация таких методов специализации системы автоматического поиска дефектов в настоящий момент является предметом исследований авторов.

Системы динамического анализа бинарного кода программ выполняют поиск дефектов (уязвимостей и некритических ошибок) путем генерации различных наборов данных и последующей передачей их на вход исследуемой программе. Возникновение исключительной ситуации, означающей наличие дефекта, отслеживается системой анализа, и текущие входные данные сохраняются для последующего воспроизведения и отладки. Кроме того, собранная информация анализируется на предмет возможности эксплуатации найденной ошибки. Уязвимости, лишь позволяющие провести атаку типа «отказ в обслуживании», считаются менее критическими, чем эксплуатируемые уязвимости, так как существуют технологии, позволяющие найти возможность для эксплуатации уязвимости и автоматической генерации взламывающей программы (эксплоита) [16, 17].

Основными задачами, которые решаются при динамическом анализе, являются: задача генерации наборов входных данных, покрывающих интересующие пути выполнения программы; запуск и трансляция программы; отслеживание возникающих уязвимостей. Часто исследование программы затрудняется применением приемов антиотладки, упаковщиков кода и навесными системами защиты от обратной инженерии. Снятие подобных защит и обход приемов антиотладки является отдельной задачей, поэтому в дальнейшем изложении будем считать, что программа не пытается препятствовать анализу.

Процесс генерации различных наборов входных данных с последующей передачей их программе получил название «фаззинг» (fuzzing), его целью является получение набора данных, выявляющих дефекты работы целевой программы. При этом не все пути исполнения программы представляют интерес, и для более интеллектуальной генерации входных данных требуется учитывать трассу выполнения программы. Для решения этой задачи программа исполняется неким транслятором, который позволяет анализировать пути выполнения, инструментировать исполняемый код или снимать трассу исполнения для последующего анализа.

Попытка сгенерировать все возможные сочетания входных данных приводит к экспоненциальному росту их объема. А значит, от транслятора требуется возможность: производить анализ выбранных или интересующих для анализа путей (например, применяя технологию символьного исполнения для некоторых путей); генерации входных данных, обеспечивающих переход по интересующим путям для увеличения покрытия; возможность параллельного запуска системы с разными входными данными для ускорения анализа.

Примером систем осуществляющих динамическую бинарную трансляцию, являются QEMU и Valgrind. QEMU — эмулятор процессоров и вычислительных систем, способен эмулировать всю вычислительную систему, в этом случае динамической трансляции подвергается код программы, все библиотеки и операционная система. В режиме эмуляции приложения транслируется только код программы и необходимые библиотеки. В свою очередь, QEMU выполняет обработку системных вызовов [18]. Valgrind является инфраструктурой для отладки и профилирования программ, в которой транслируется лишь пользовательская программа в том же окружении, что и при обычном выполнении. Valgrind включает в себя ряд инструментов, реализованных поверх базовой инфраструктуры трансляции, самым популярным из которых является Memcheck, ориентированный для анализа утечек памяти и обращений к невыделенной памяти, позволяет транслировать программу в промежуточное представление, находящееся в SSA-форме, затем код инструментируется и транслируется в машинный код [19].

KLEE — инструмент для символьного исполнения [20], анализ производится над внутренним представлением компиляторной инфраструктуры LLVM [21]. Инструмент позволяет запускать «символьные» процессы, при этом в ходе интерпретации инструкции внутреннего представления LLVM отображаются в систему уравнений, которые затем решаются с использованием инструмента STP [22] для получения новых путей выполнения, которые требуется обойти. Для ускорения анализа система позволяет выполнять несколько путей одновременно.

S2E — система выборочного символьного исполнения, построенная на базе QEMU и KLEE. S2E основывается на двух базовых идеях: выборочном символьном выполнении, позволяющем автоматически минимизировать количество кода, который будет исполнен символьно, и модели консистентности, обеспечивающей при анализе контроль баланса производительность/точность. Ключевые возможности системы заключаются в одновременном анализе нескольких путей, возможности анализа всей системы (программ пользователя, библиотек, ядра, драйверов), возможность анализа бинарного кода [23].

Avalanche — система динамического анализа, разрабатываемая в ИСП РАН [24]. Avalanche решает задачи отслеживания уязвимостей в ходе выполнения программы и интеллектуальной генерации входных данных для увеличения покрытия путей через собственные инструменты на основе инфраструктуры Valgrind и упомянутый решатель STP. Для поддержки языка Java используется статическая инструментация кода, но сохраняется общая схема итеративного динамического анализа.

Mayhem — система автоматического поиска эксплуатируемых уязвимостей в бинарном коде [25]. Каждая найденная уязвимость сопровождается рабочим эксплоитом. Ключевые особенности инструмента: гибридное онлайн-оффлайн исполнение кода, эмуляция на уровне приложения, а не всей системы, набор различных эвристик для работы с символьными указателями. Система основана на инфраструктуре двоичной трансляции PIN [26], обеспечивающей инструментирование бинарного кода, для перевода во внутреннее представление используется BAP [27], в качестве решателя используется Z3 [28].

Таким образом, системы динамического анализа представляют совокупность нескольких модулей-инструментов (зачастую, с открытым исходным кодом), решающих основные сформулированные задачи анализа. Экспоненциальная сложность анализа и применения в случае нетривиальных алгоритмов обработки входных данных и/или модели исполнения (например, обратные вызовы процедур на мобильных платформах) преодолевается новыми эвристиками, позволяющими производить более глубокий анализ программы.

**Список литературы**

1. Аветисян А.И. Современные методы статического и динамического анализа программ для решения приоритетных проблем программной инженерии: автореф. дис. … д-ра физ.-мат. наук: 05.13.11/Аветисян Арутюн Ишханович. М., 2011. 36 с.

2. Марков А.С. Немонотонные модели оценки надежности и безопасности функционирования программных средств на ранних этапах испытаний. Научно-практический журнал «Вопросы кибербезопасности». М.: ОАО «НПО «Эшелон». ISNB2311–3456. 2014. № 2 (3). С. 10–17.

3. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства. Научно-практический журнал «Вопросы кибербезопасности». М.: ОАО «НПО «Эшелон». ISNB2311–3456. 2014. № 1 (2). С. 13–22.

4. Чукляев И.И., Морозов А.В., Болотин И.Б. Теоретические основы построения адаптивных систем комплексной защиты информационных ресурсов распределенных информационно-вычислительных систем: монография. Смоленск: ВА ВПВО ВС РФ, 2011. 227 с.

5. Морозов А.В., Чукляев И.И. Информационная безопасность вычислительных систем боевого управления в аспекте информационного противоборства. Научно-практический журнал «Проблемы безопасности российского общества». М.: МГУПС. ISNB2307–4396. 2013. № 2–3. С. 85–91.

6. База Common Weakness Enumeration. Режим доступа: http://cwe.mitre.org.

7. База Common Vulnerabilities and Exposures. Режим доступа: http://cve.mitre.org.

8. Gallaher M.P. and Kropp B.M. Economic impacts of inadequate infrastructure for software testing. Technical report, RTI International, National Institute of Standards and Technology, US Dept of Commerce, May 2002.

9. Forrest Shull, Vic Basili, Barry Boehm, Winsor A. Brown, Patricia Costa, Mikael Lindvall, Dan Port, Ioana Rus, Roseanne Tesoriero, and Marvin Zelkowitz. What we have learned about fighting defects. In International Software Metrics Symposium. Ottawa, Canada, 2002.

10. Klocwork Insight. Системы анализа исходного кода [Электронный ресурс]. Режим доступа: http://www.klocwork.com/products.

11. Coverity. Static source code analysis solutions [Электронный ресурс]. Режим доступа: http://www.coverity.com.

12. GrammaTech, Inc. CodeSonar [Электронный ресурс]. Режим доступа: http://www.grammatech.com/products/codesonar/overview.html.

13. Аветисян А.И., Белеванцев А.А., Бородин А.Е., Несов В. Использование статического анализа для поиска уязвимостей и критических ошибок в исходном коде программ. Труды ИСП РАН Т. 2011. 21. С. 23–38.

14. Аветисян А.И., Бородин А.Е. Механизмы расширения системы статического анализа Svace детекторами новых видов уязвимостей и критических ошибок. Труды ИСП РАН. 2011. Т. 21. С. 39–54.

15. Иванников В.П., Белеванцев А.А., Бородин А.Е., Игнатьев В.Н., Журихин Д.М., Аветисян А.И., Леонов М.И. Статический анализатор Svace для поиска дефектов в исходном коде программ. Труды ИСП РАН том 26. 2014. Вып. 1. С. 231–250.

## THE MODERN TECHNOLOGIES OF STATIC AND DYNAMIC ANALYSIS OF SOFTWARE

**Chuklyaev Eugenii Igorevich,**
Smolensk, Russia, smolrsu@mail.ru

**Abstract**
The article presents the results of an analysis of existing approaches protect and identify defects (vulnerabilities and errors) in the source and binary codes programs conducted at various stages of their development, design and operation. Summarizes the most common defects in the code and objects of influence, functional and ergonomic requirements for a modern system of analysis.

**Keywords:** static and dynamic analysis; source and binary code; defects (vulnerabilities and bugs); requirements; security technologies; facilities tampering.

**References**
1. Avetisyan AI Modern methods of static and dynamic analysis of programs to address priority issues of software engineering: Author. Dis... Dr. Sci. Sciences: 05.13.11 / Harutyun Avetisyan Ishhanovich. Moscow, 2011. 36 p.
2. A. Markov model Nonmonotone assess the reliability and safety of software in the early stages of testing. Scientific and practical journal "Issues of cybersecurity." Moscow, "NPO" Echelon ". ISNB2311–3456. 2014. No. 2 (3). Pp. 10–17.
3. Makarenko SI Chuklyaev II terminological basis in the field of information warfare. Scientific and practical journal "Issues of cybersecurity." Moscow, "NPO" Echelon ". ISNB2311–3456. 2014. No. 1 (2). Pp. 13–22.
4. Chuklyaev I.I., Morozov V., Bolotin I.B. Theoretical bases of construction of complex adaptive systems to protect information resources of distributed information systems: monograph. Smolensk: BA VPVO Armed Forces, 2011. 227 p.
5. Morozov A.V., Chuklyaev I.I. Information security of computer systems in the command and control aspect of information warfare. Scientific and practical journal "Problems of security of the Russian society." Moscow, MGUPS. 2013. No. 2–3. Pp. 85–91.
6. Base Common Weakness Enumeration. URL: http://cwe.mitre.org.
7. Base Common Vulnerabilities and Exposures. URL: http://cve.mitre.org.
8. Gallaher M.P., Kropp B.M. Economic impacts of inadequate infrastructure for software testing. Technical report, RTI International, National Institute of Standards and Technology, US Dept of Commerce, May 2002.
9. Forrest Shull, Vic Basili, Barry Boehm, Winsor A. Brown, Patricia Costa, Mikael Lindvall, Dan Port, Ioana Rus, Roseanne Tesoriero, and Marvin Zelkowitz. What we have learned about fighting defects. In International Software Metrics Symposium. Ottawa, Canada, 2002.
10. Klocwork Insight. System source code analysis. URL: http://www.klocwork.com/products.
11. Coverity.Static source code analysis solutions. URL: http://www.coverity.com.
12. GrammaTech, Inc. CodeSonar. URL: http://www.grammatech.com/products/codesonar/overview.html.
13. Avetisyan A.I., Belevantsev A., Borodin A.E., Nessov B. Using static analysis to find vulnerabilities and critical errors in the source code of programs.Proceedings of ISP RAS is 21. 2011. Pp. 23–38.
14. Avetisyan A.I., Borodin A.E. extension mechanism of static analysis Svace detectors of new types of vulnerabilities, and critical errors. ISPRAS Proceedings. 2011. Vol. 21. Pp. 39–54.
15. Ivannikov V.P., Belevantsev A.A., Borodin A.E., Ignatiev V.N., Zhurikhin D.M., Avetisyan A.I., Leonov M.I. A static analyzer Svace to find defects in the source code of programs.Proceedings ISPRAS that 26. 2014. Vol. 1. Pp. 231–250.

**Information about author:**
Chuklyaev E. I., Researcher Smolensk public organization to promote science and education "Regional Union of Scientists", Smolensk, Russia.

# СТРУКТУРА МОДЕЛИ МЕХАНИЗМА ФОРМИРОВАНИЯ УПРАВЛЯЮЩИХ ВОЗДЕЙСТВИЙ НА СПЕЦИАЛИСТОВ БОЕВЫХ СРЕДСТВ ЗЕНИТНЫХ КОМПЛЕКСОВ

**Голов Евгений Григорьевич**,
*адъюнкт 9 кафедры (зенитных комплексов ближнего действия) Военной академии войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М.Василевского, г. Смоленск, Россия, golov.82@yandex.ru*

**Аннотация**
Постановка проблемы: проведение исследований предусматривало выработку требований, предъявляемых к структуре и содержанию модели механизма формирования управляющих воздействий на специалистов боевых средств зенитных комплексов в интересах повышения эффективности боевой подготовки. В работе проведено обоснование необходимости использования модели механизма формирования управляющих воздействий на на специалистов боевых средств зенитных комплексов, за счёт использования ее в программном обеспечении УТС с применением соответствующих моделей на основе единой базы данных, созданной с учётом требований директивных (нормативных) документов об организации боевой подготовки подразделений, вооружённых ЗК, эксплуатационной документацией предприятий-изготовителей ЗК и экспертных оценок специалистов в области эксплуатации и боевого применения ЗК.

**Ключевые слова:** *модель механизма формирования управляющих воздействий; система поддержки принятия решений; специалисты боевых средств зенитных комплексов; учебно-тренировочные средства, лицо принимающее решения; вариант управляющих воздействий; блок нечеткого вывода.*

Разработанная методика повышения уровня подготовленности специалистов боевых средств зенитных комплексов (БС ЗК) (рис. 1) [1] может быть реализована за счёт разработки и последующего использования в программном обеспечении современных и перспективных учебно-тренировочных средствах (УТС) соответствующей модели (рис. 2).

Предлагаемая модель в полной мере основывается на единой базе данных, созданной с учётом требований директивных (нормативных) документов об организации боевой подготовки подразделений, вооружённых ЗК БД, эксплуатационной документации предприятий-изготовителей ЗК БД и экспертных оценок специалистов по боевому применению и эксплуатации этих комплексов [2].

На рис. 2: $X_{u_N}$ — множество значений итоговых оценок деятельности специалиста БС ЗК за $N$-е количество стрельб; $Y$ — значение оценки уровня подготовленности специалистов БС ЗК по результатам $N$-о количества стрельб; $\{X_ч\}$ — множество частных оценок специалистов БС ЗК за $N$-е количество стрельб; $X_{k1}$ — оценка за качество выполнения операций (процедур) боевой работы при стрельбе по воздушной цели (ВЦ); $X_{k2}$ — количественная оценка за результат стрельбы по ВЦ с учётом допущенных нарушений правил стрельбы, $Y_u$ — оценка уровня подготовленности обучаемого специалиста; $Q_{сп}$ — категория обучаемого специалиста БС ЗК; $T_{упр}$ — тип упражнений из состава базы данных; $P_{упр}$ — сложность предлагаемых упражнений; $J_{упр}$ — количество упражнений; $\{Z_{пр}\}$ — предварительный вариант управляющих воздействий; $\{Z_u\}$ — итоговый вариант управляющих воздействий на специалиста БС ЗК; $L_{ЛПР}$ — степень вмешательства лица принимающего решения (ЛПР) в формировании итогового варианта управляющих воздействий.

Разработка модели автоматизированной СППР для специалистов БС ЗК, ключевым звеном которой является механизм формирования управляющих воздействий на специалистов БС ЗК, включает несколько этапов, базирующихся на известной методике моделирования нечётких экспертных управляющих систем, в числе которых — выбор механизма разработки продукционных правил и вида базовых функций принадлежности входных и выходных переменных [3].

Входными данными для модели автоматизированной СППР для специалистов БС ЗК являются данные, полученные с использованием апробированной модели автоматизированной оценки деятельности специалистов БС ЗК, которая разработана с использованием усовершенствованной методики оценивания боевой работы операторов зенитных комплексов войсковой ПВО с определением уровня подготовленности. Данная модель была разработана в ходе научных исследований кандидатами технических наук Андреевым С.Г. и Семенко И.Б.

Модель позволяет осуществлять фиксацию категорий ошибок и их количества за выполнение отдельных операций (процедур) боевой работы, в результате чего, позволяет сформировать соответствующие частные оценки, которые определяют значения итоговой оценки обучающемуся специалисту.

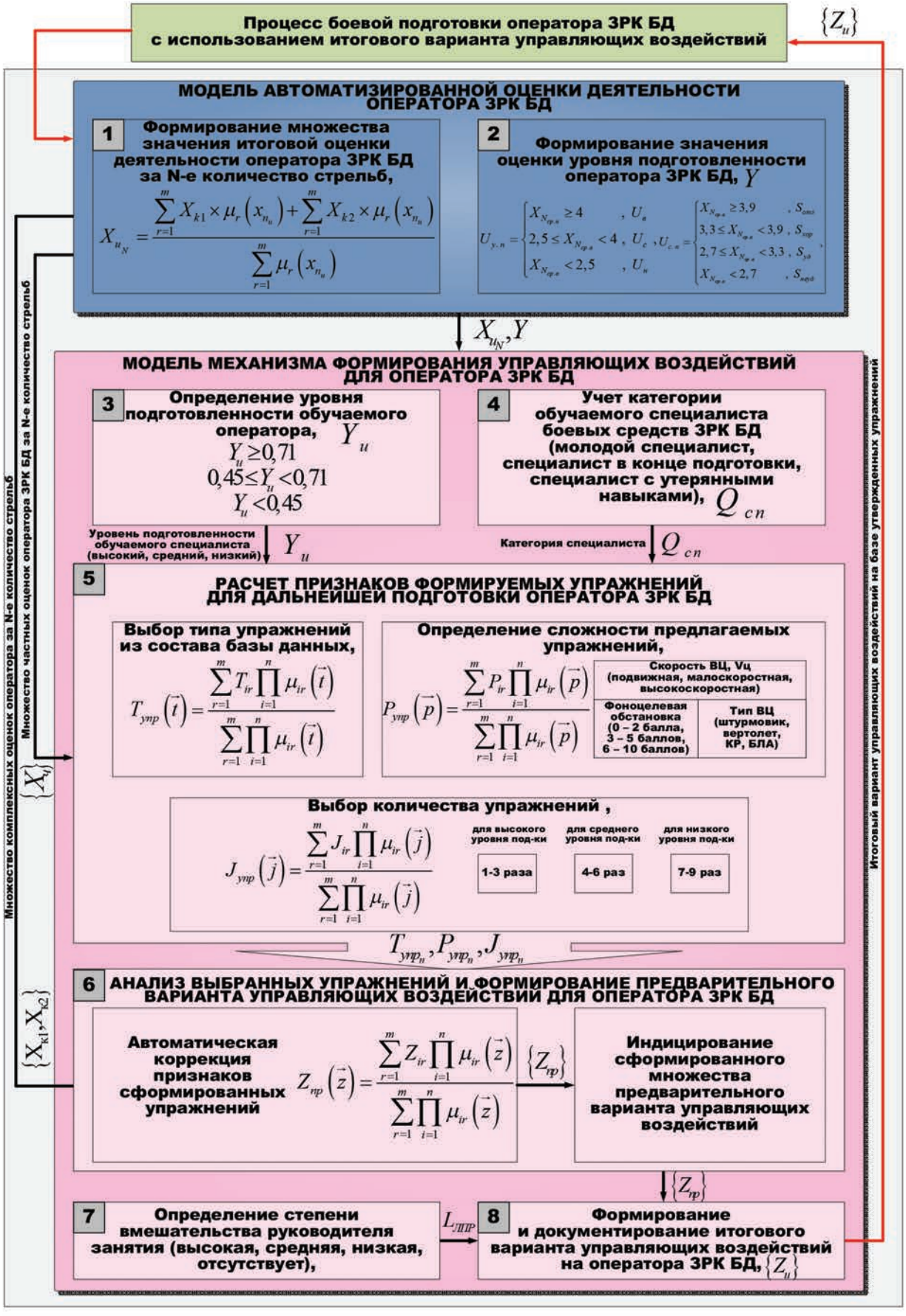



**Рис. 1.** Методика повышения уровня подготовленности специалистов боевых средств зенитных комплексов

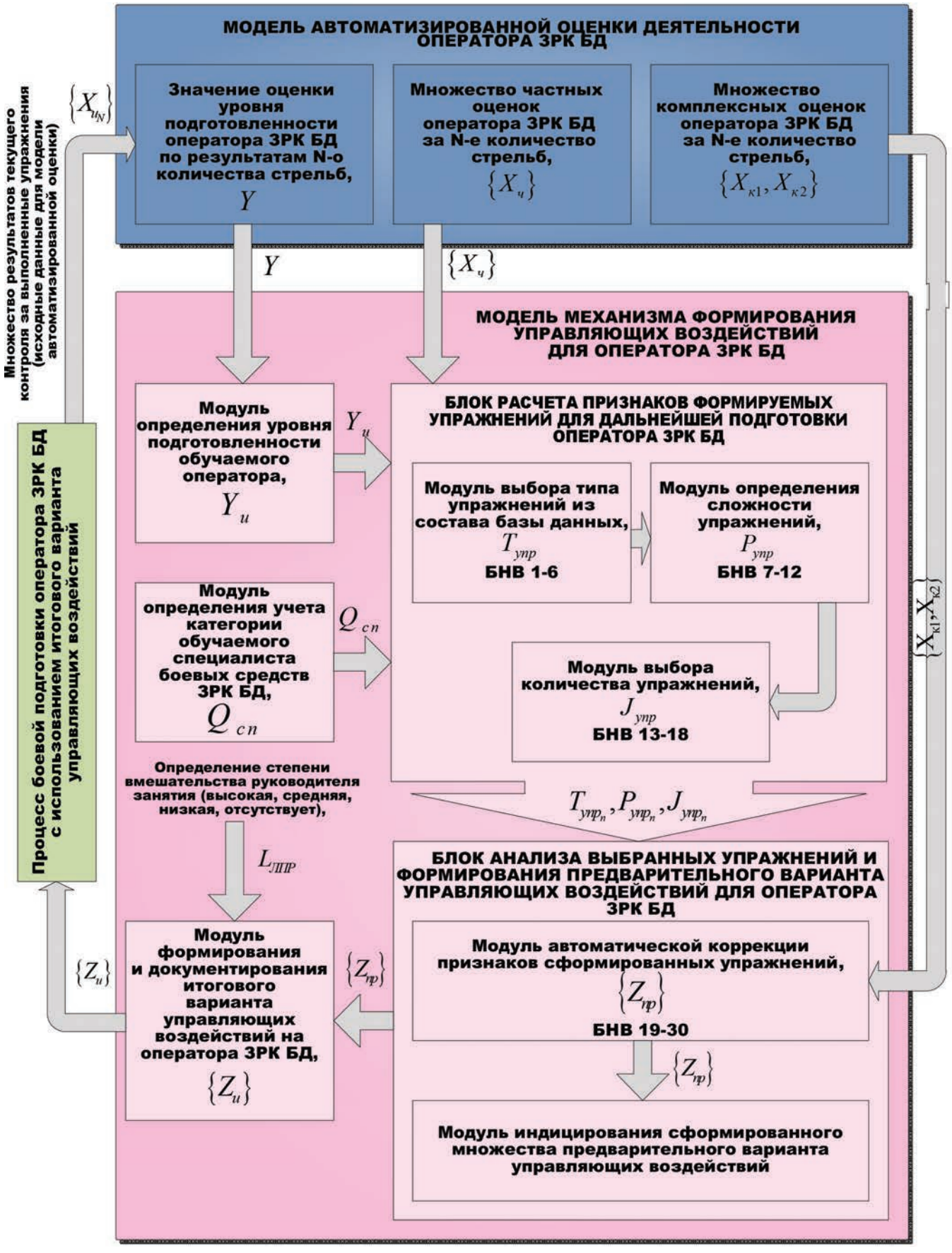



**Рис. 2.** Структура модели автоматизированной СППР для специалистов боевых средств зенитных комплексов

Величина итоговой оценки боевой работы оператора определяется с учётом значений комплексных оценок $X_{k1}$ и $X_{k2}$.

Так же эта модель реализует автоматизированное формирование оценки уровня подготовленности специалистов БС ЗК с учетом условий стрельбы (состояние фоноцелевой обстановки, скорости движения ВЦ) для каждого конкретного пуска зенитной управляемой ракеты (ЗУР).

Всё это позволяет значительно повысить качество оценки специалистов БС ЗК в ходе стрельб на существующих и перспективных ЗК, обеспечивая проведение точного и эффективного анализа результатов занятий и стрельб с ними в целях формирования эффективных управляющих воздействий на военнослужащих, что в конечном итоге положительно скажется на процессе боевой подготовки подразделений, вооружённых ЗК, и приведёт к увеличению эффективности стрельбы ЗК.

Используя частные оценки за выполнение всего множества операций (процедур) боевой работы операторов при стрельбе по ВЦ, комплексные и итоговую оценку, а так же значения оценки уровня подготовленности специалистов БС ЗК возможно определить необходимые управляющие воздействия на специалиста БС ЗК для дальнейшей его боевой подготовки. Это является основным предназначением разработанной модели механизма формирования управляющих воздействий на специалистов БС ЗК в перспективной СППР (рис. 2).

Разработка модели механизма формирования множества управляющих воздействий при подготовке специалистов БС ЗК в специализированной СППР, реализованной на базе УТС, базируется на методике моделирования нечётких экспертных систем [4].

В соответствии с единой базой данных упражнений и используя методику повышения уровня подготовленности специалистов БС ЗК (рисунок 1), разработана структура модели механизма формирования множества управляющих воздействий на специалистов БС ЗК, представленная на рисунке 3.

С выхода этой модели $\{Z_u\}$ итоговый вариант управляющих воздействий на специалистов БС ЗК непосредственно используется в процессе боевой подготовки специалистов БС ЗК.

В связи с тем, что в основе применяемых в модели блоков нечеткого вывода (БНВ) используется алгоритм Сугэно нулевого порядка, функции выходных переменных (на примере БНВ модуля выбора типа упражнений) могут быть определены как константы в виде целых чисел («1», «2», «3», «4», «5» и «6»), по сути являющиеся номерами управляющих воздействий, определяющих тип упражнений из состава варианта специализированной базы данных для специалистов БС ЗК.

Таким образом, продукционные правила нечётких систем в формальном виде могут быть представлены типовым условием

$$\Pi_r\text{: если } t_1 \text{ есть } F_{r1} \text{ и } t_2 \text{ есть } F_{r2}, \ldots, t_u \text{ есть } F_{ru}, \text{ то } T_i = T_j,$$

где $F_{r1}, F_{r2}, \ldots, F_{ru}$ — нечёткие числа, описываемые треугольными (трапецеидальными) функциями принадлежности;

$j = 1, 2, \ldots, x$ — количественное значение номера типа упражнения в соответствии с базой данных упражнений;

$x$ — количество упражнений в соответствии с базой данных;

$r = 1, 2, \ldots, m$ — номер продукционного правила нечёткой системы;

$m$ — количество продукционных правил нечёткой системы;

$T_i$ — постоянный параметр;

$T_j$ — номер упражнения.

Следует отметить, что параметры продукционных правил выбираются при экспертной оценке в процессе формирования априорной базы знаний.

Формирование совокупности нечетких продукционных правил и выбор вида функций принадлежности подразумевают определение необходимого количества продукционных правил, например, на множестве $\{F\}$ [5]. С этой целью необходимо разбить диапазон определённых базой знаний типов упражнений по уровням сложности на отдельные интервалы для каждого [2].

Таким образом, с учётом вышепредложенного подхода формируются продукционные правила определения сложности, количества упражнений, предлагаемых специалисту БС ЗК, а так же продукционные правила определения предварительного варианта управляющих воздействий с целью его дальнейшего использования в модели механизма формирования управляющих воздействий для специалистов БС ЗК.

Очевидно, что применение в нечёткой системе алгоритма нечёткого вывода на базе алгоритма Сугэно нулевого порядка позволяет решить задачу определения на множестве $\{T\}$ тип упражнений со своим набором операций (процедур) боевой работы предлагаемых специалисту, определённых базой данных, за счёт использования в модели формирования управляющих воздействий БНВ как при формировании типа, сложности и количества упражнений так и при формировании предварительного варианта управляющих воздействий для специалистов, что, в свою очередь, даёт возможность достоверно и объективно сформировать итоговый вариант управляющих воздействий для специалистов для их дальнейшего процесса боевой работы.

Структура разработанной модели (рис. 3) позволяет максимально учесть «человеческий фактор» и минимизировать связанные с его проявлением ошибки при формировании итогового варианта управляющих воздействий для специалистов БС ЗК для их дальнейшего процесса боевой работы при стрельбе по ВЦ на УТС.

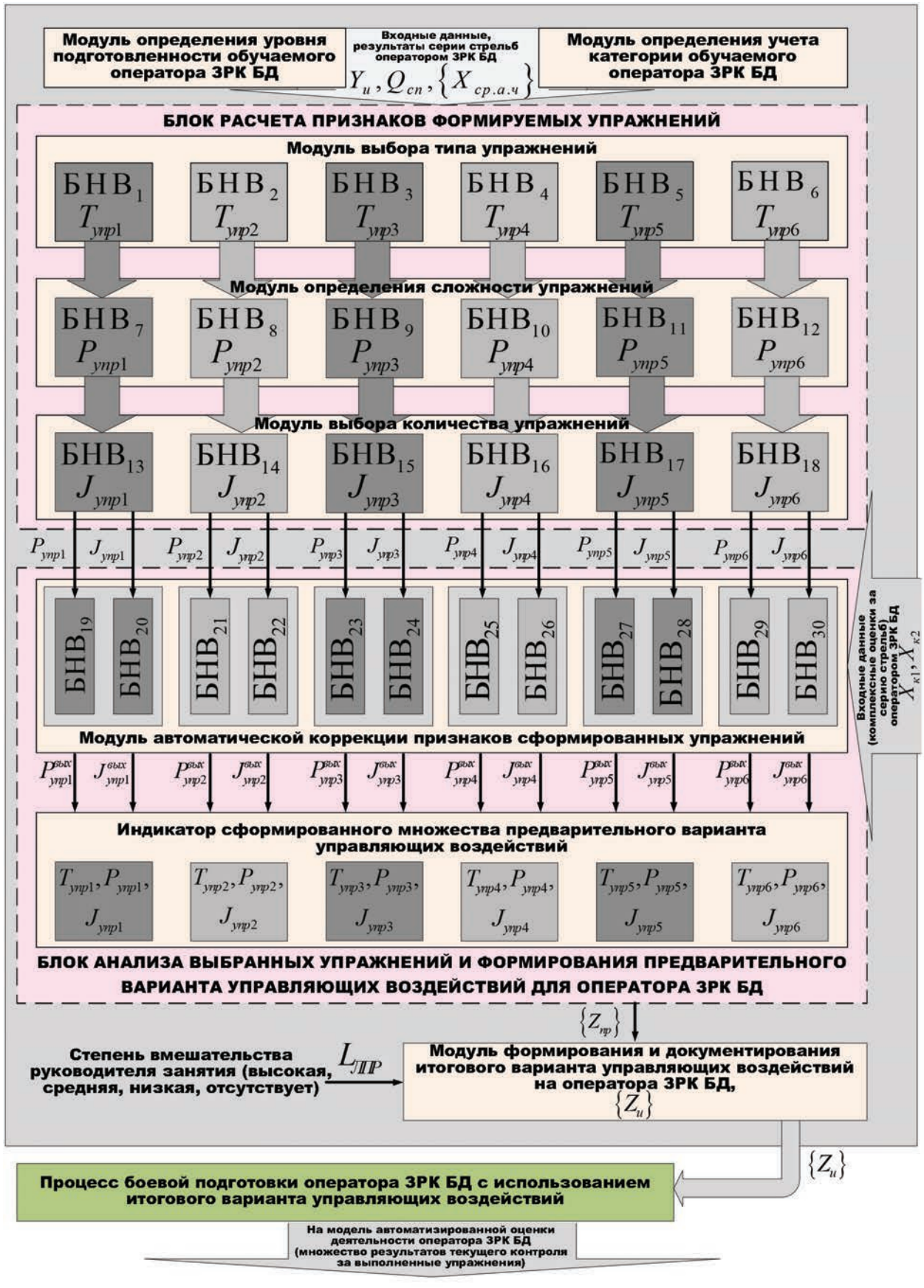



**Рис. 3.** Структура модели механизма формирования управляющих воздействий специалистов боевых средств зенитных комплексов

Значения входных переменных: $Y_u$ — уровень подготовленности обучаемого оператора, $Q_{сп}$ — учет категории обучаемого специалиста БС ЗК, $\{X_ч\}$ — среднее арифметическое частных оценок специалиста БС ЗК за $N$-е количество стрельб поступают в блок расчета признаков формируемых упражнений для дальнейшей подготовки специалистов БС ЗК.

В блоке расчета признаков формируемых упражнений для дальнейшей подготовки специалистов БС ЗК предлагаемой модели в трех модулях проводится определение типа, сложности и количества упражнений предлагаемых специалисту.

Используя разработанный вариант структуры базы данных упражнений для обучаемых специалистов БС ЗК, специалисту предлагается шесть типов упражнений со своим набором тренируемых операций боевой работы. В модуле выбора типа упражнений из состава базы данных с использованием $БНВ_1$ — $БНВ_6$ определяется необходимость выполнять данные типы упражнений оператору. Типы упражнений пронумерованы соответственно с первого по шестой. На выходе модуля выбора типа упражнений будут индицироваться номера типов выбранных упражнений, упражнения, в которых оператор не допускает ошибок и соответственно, которые не будут предлагаться ему для отработки будут обозначаться цифрой «ноль».

На входы БНВ с поступают множества $Y_u$, $Q_{сп}$, $\{X_ч\}$ «нечётко связанных» показателей. При этом функциональная зависимость типа упражнения, формируемой БНВ, описывается выражением:

$$T_{упр}\left(\vec{t}\right) = \frac{\sum_{r=1}^{m} T_{ir} \prod_{i=1}^{n} \mu_{ir}\left(\vec{t}\right)}{\sum_{r=1}^{m} \prod_{i=1}^{n} \mu_{ir}\left(\vec{t}\right)} \tag{1}$$

где $\vec{t} = \{t_1, t_2, ..., t_n\}$ — множество входных переменных;

$\mu_r(\vec{t}) = \mu_{r1}(t_1) \cdot \mu_{r2}(t_2) \cdot ... \cdot \mu_{rn}(t_n)$ — совокупность функций входных переменных;

$i = 1, 2, \ldots, n$ — номер оцениваемого входного воздействия;

$n$ — количество оцениваемых входных воздействий (входных переменных);

$r = 1, 2, \ldots, m$ — номер продукционного правила нечёткой системы;

$m$ — количество продукционных правил нечёткой системы;

$T_{ir}$ — тип упражнения i-ого входного воздействия.

Далее в следующем модуле определения сложности упражнений с использованием $БНВ_7$ — $БНВ_{12}$ определяется сложность выбранных упражнений предложенных для отработки оператору. Введены 3 уровня сложности упражнений:

– низкий уровень сложности упражнений, индицируется на соответствующих индикаторах под цифрой «1»;

– средний уровень сложности упражнений, индицируется на соответствующих индикаторах под цифрой «2»;

– высокий уровень сложности упражнений, индицируется на соответствующих индикаторах под цифрой «3»;

Определение уровня сложности предлагаемых упражнений, $P_{упр}$ для дальнейшей подготовки специалистов БС ЗК, происходит путем определения конкретных упражнений для выполнения в ходе дальнейшей боевой подготовки, с учетом их уровня сложности. Уровень сложности упражнений может выбираться по трем составляющим: скорость воздушной цели (подвижная, неподвижная), фоноцелевая обстановка (измеряется в баллах от одного до десяти), тип воздушной цели (штурмовик, вертолет, крылатая ракета (КР), беспилотный летательный аппарат (БЛА). Так например, специалисту, имеющему низкий уровень подготовленности будет соответствовать такой уровень сложности упражнений, в котором:

– типом воздушной цели будет являться вертолет;

– скорость воздушной цели будет менее 1 м/с, то есть ВЦ неподвижна;

– фоноцелевая обстановка будет находится в пределах от 0 до 2 баллов, что соответствует ясной, безоблачной погоде, ведению боевой работы в безпомеховой обстановке, в пустынной (степной) местности и т. п.;

специалисту, имеющему высокий уровень подготовленности, будет соответствовать уровень сложности упражнений в котором:

– типом воздушной цели будет являться штурмовик, КР или БЛА;

– скорость воздушной цели будет более 1 м/с (подвижная ВЦ);

– фоноцелевая обстановка будет находится в пределах от 6 до 10 баллов, что соответствует фоновой обстановке с резкими разрывами в облаках, подсвечиваемые солнцем, ведение боевой работы в условиях применения противником помех, в горной, лесистой местности, в тёмное время суток и т. п.

Соответственно специалисту, имеющему средний уровень подготовленности, будет соответствовать уровень сложности упражнений со средними значениями.

На входы БНВ так же поступают множества $Y_u$, $Q_{сп}$, $\{X_ч\}$ «нечётко связанных» показателей. При этом математическое описание процесса формирования сложности упражнений, формируемого БНВ, описывается выражением:

$$P_{упр}\left(\vec{p}\right) = \frac{\sum_{r=1}^{m} P_{ir} \prod_{i=1}^{n} \mu_{ir}\left(\vec{p}\right)}{\sum_{r=1}^{m} \prod_{i=1}^{n} \mu_{ir}\left(\vec{p}\right)} \tag{2}$$

Следующий модуль выбора количества упражнений из состава блока расчета признаков формируемых упражнений (приложение Г) определяет количество выбранных упражнений специалисту БС ЗК $J_{\text{упр}}$. При этом очевидно, что чем ниже уровень подготовленности обучаемого специалиста, тем большее количество упражнений ему необходимо для дальнейшего обучения. Определение количества упражнений происходит по следующим параметрам: при высоком уровне подготовленности специалиста БС ЗК количество упражнений будет равно 1–3 раза; при среднем уровне подготовленности количество упражнений будет равно 4–6 раз; соответственно низкому уровню подготовленности специалиста БС ЗК количество упражнений будет равно 7–9 раз. Количество упражнений индицируется на соответствующих индикаторах соответственно цифрами «1», «2», «3», «4», «5», «6», «7», «8», «9».

Входными данными на БНВ являются те же множества $Y_{\text{ц}}$, $Q_{\text{сп}}$, $\{X_{\text{ч}}\}$ «нечётко связанных» показателей. Математическое описание процесса формирования количества упражнений, формируемого БНВ, описывается выражением:

$$J_{\text{упр}}\left(\vec{j}\right) = \frac{\sum_{r=1}^{m} J_{ir} \prod_{i=1}^{n} \mu_{ir}\left(\vec{j}\right)}{\sum_{r=1}^{m} \prod_{i=1}^{n} \mu_{ir}\left(\vec{j}\right)} \tag{3}$$

В результате в блоке расчета признаков формируемых упражнений сформирован набор необходимых для дальнейшей подготовки специалиста БС ЗК упражнений соответствующего типа, уровня сложности и их количества.

Но для более точного определения сложности и количества предложенных специалисту БС ЗК упражнений необходимо учитывать полученные им при стрельбе по ВЦ на УТС величины предварительных (комплексных оценок): $X_{k1}$ — оценка за качество выполнения операций (процедур) боевой работы при стрельбе по ВЦ; $X_{k2}$ — количественная оценка за результат стрельбы по ВЦ с учётом допущенных нарушений правил стрельбы.

Решением данной проблемы является использование модуля автоматической коррекции признаков сформированных упражнений, входящий в состав блока анализа выбранных упражнений и формирования предварительного варианта управляющих воздействий для специалиста БС ЗК (рис. 3).

В модуле автоматической коррекции признаков сформированных упражнений с использованием $\text{БНВ}_{19}$ — $\text{БНВ}_{30}$ производится автоматическая коррекция сложности и количества упражнений, предложенных специалисту. Входными данными на БНВ являются множества $X_{k1}$, $X_{k2}$ — количественная и качественная оценки полученные специалистом БС ЗК за серию стрельб на УТС, а так же сформированные данные (сложность и количество упражнений) в блоке расчета признаков формируемых упражнений. В результате с выхода модуля автоматической коррекции признаков сформированных упражнений на индикатор сформированного множества предварительного варианта управляющих воздействий поступят 6 трехзначных цифровых набора, определяющих необходимые упражнения (тип, сложность и количество) для дальнейшей боевой подготовки специалиста БС ЗК. Первая цифра обозначает выбранный номер и тип упражнения от одного до шести; вторая цифра обозначает сложность выбранного типа упражнения от одного до трех; третья цифра обозначает какое количество раз данный тип упражнения данного уровня сложности необходимо выполнить специалисту БС ЗК.

В итоге эти данные индицируются на соответствующем индикаторе и предлагаются ЛПР (руководителю занятия) для анализа. ЛПР проанализировав эти данные, определяет степень своего вмешательства, $L_{\text{ЛПР}}$ (высокая, средняя, низкая, отсутствует). В соответствии с этим определение степени вмешательства ЛПР будет соответствовать тому, что:

ЛПР откажется от предложенных упражнений, и самостоятельно выберет необходимые упражнения для дальнейшей подготовки обучаемого специалиста БС ЗК (специалист будет отрабатывать упражнения, предложенные руководителем занятия (тренажа);

ЛПР согласится с предложенными упражнениями, но внесет значительную их корректировку (специалист БС ЗК будет отрабатывать упражнения, предложенные механизмом формирования управляющих воздействий, но значительно отредактированных руководителем занятия (тренажа);

ЛПР согласится с предложенными упражнениями, но внесет незначительную их корректировку (специалист БС ЗК будет отрабатывать упражнения, предложенные механизмом формирования управляющих воздействий, но незначительно отредактированных руководителем занятия (тренажа);

ЛПР согласится с предложенными упражнениями (специалист БС ЗК будет отрабатывать упражнения, предложенные механизмом формирования управляющих воздействий).

В конечном итоге будет сформирован итоговый вариант управляющих воздействий на обучаемого специалиста БС ЗК, $Z_{\text{u}}$ с учетом вмешательства ЛПР. Итоговый вариант управляющих воздействий после документирования исходных данных, предназначенных для визуализации и документирования процесса оценивания результатов стрельб ЗК на УТС и формирования оптимального множества управляющих воздействий на обучаемых специалистов БС ЗК в целях оказания помощи ЛПР в принятии решений в ходе дальнейшей боевой подготовки подразделений будет предложен специалисту БС ЗК для его дальнейшей боевой подготовки.

**Вывод**

Использование разработанной автоматизированной модели механизма формирования управляющих воздействий на специалистов БС ЗК (рисунок 2) в специализированной СППР, реализованной на базе УТС существенно повысит качество подготовки специалистов БС ЗК. Это обеспечивается за счёт увеличения значения коэффициента уровня подготовленности обучаемых, что в конечном итоге повысит эффективность ЗК в целом. Таким образом модель механизма формирования управляющих воздействий на специалистов БС ЗК может быть использована в интересах совершенствования программного обеспечения УТС современных и перспективных ЗК.

**Список литературы**

1. Голов Е.Г. Методика повышения Уровня подготовленности специалистов зенитных комплексов ближнего действия // Сборник материалов VII международной молодежной конференции. 2015. С. 176–178.

2. Усков А.А. Моделирование систем управления в среде MATLAB // Проектирование АСОИУ и Моделирование систем. Смоленск: СФ МЭИ (ТУ). 2003. 35 с.

3. Круглов В.В., Дли М.И., Голунов Р.Ю. Нечёткая логика и искусственные нейронные сети. М.: Издательство Физико-математической литературы. 2001. 224 с.

4. Круглов В.В., Борисов В.В. Гибридные нейронные сети. Смоленск: Русич. 2001. 224 с.

5. Кричевский М.Л. Интеллектуальный анализ данных в менеджменте. СПб.: СПбГУАП, 2005. 208 с.

## STRUCTURE OF MODEL OF THE MECHANISM OF FORMATION OF MANAGING DIRECTORS OF IMPACTS ON EXPERTS OF MEANS OF WAR OF SURFACE-TO-AIR MISSILE SYSTEMS

**Golov Evgeny Grigoryevich,**
Smolensk, Russia, golov.82@yandex.ru

**Abstract**

Problem statement: carrying out researches provided development of the requirements shown to structure and the maintenance of model of the mechanism of formation of operating impacts on experts of means of war of surface-to-air missile systems in interests of increase of efficiency of combat training.

In work justification of need of use of model of the mechanism of formation of managing directors of influences on experts of means of war of surface-to-air missile systems, at the expense of its use in EDUCATIONAL TRAINING MEANS (ETM) software with application of the corresponding models on the basis of the uniform database created taking into account requirements of directive (standard) documents on the organization of combat training of divisions, armed surface-to-air missile systems, operational documentation of surface-to-air missile systems manufacturers and expert estimates of experts in the field of operation and fighting application of surface-to-air missile systems is carried out.

**Keywords:** model of the mechanism of formation of operating influences; system of support of decision-making; experts of means of war of surface-to-air missile systems; educational and training means; the person making decisions; option of operating influences; the block of an indistinct conclusion.

**References**

1. Golov E.G. Technique of increase of Level of readiness of experts of short-range surface-to-air missile systems / Collection of materials VII of the international youth conference. 2015. Pp. 176-178.

2. Uskov A.A. Modeling of control systems in the environment of MATLAB. Design the automated systems of processing of information and management and modeling of systems. Smolensk: SF MEI (TU). 2003. 35 p.

3. Kruglov V. V., Dli M. I., Golunov R.Yu. Indistinct logic and artificial neural networks. Moscow: Publishing house of Physical and mathematical literature. 2001. 224 p.

4. Kruglov V. V., Borisov V.V. Hybrid neural networks. Smolensk: Rusich. 2001. 224 p.

5. Krichevsky M. L. The intellectual analysis of data in management. St-Petersburg.: SPbGUAP, 2005. 208 p.

**Information about author:**

Golov E.G., postgraduate student 9 chairs (short-range surface-to-air missile systems) Military academy of army antiaircraft defense of Armed forces of the Russian Federation of a name of the Marshal of the Soviet Union of A.M.Vasilevsky.

# УСКОРЕНИЕ СХОДИМОСТИ ПРОЦЕССА ОБРАБОТКИ ТРАЕКТОРНЫХ ИЗМЕРЕНИЙ КОСМИЧЕСКИХ АППАРАТОВ НА ОРБИТАХ ТИПА «МОЛНИЯ» ПРИ ВЫСОКИХ ПОГРЕШНОСТЯХ НАЧАЛЬНОГО ПРИБЛИЖЕНИЯ

**Доронкин Алексей Валерьевич,**
*инженер-исследователь 1 категории ОАО «Корпорация «Комета», г. Москва, Россия, bj13@yandex.ru*

**Аннотация**
Предложена методика обработки разноточных траекторных измерений космических аппаратов (КА) на орбитах типа «Молния», базирующаяся на анализе свойств линейности многомерной функции связи измеряемых и оцениваемых параметров. Посредством проведенного статистического моделирования установлено, что использование предложенной методики позволяет существенно повысить точность начального приближения, используемого для проведения итерационных расчетов оценивания параметров орбиты КА. Показано, что это обеспечивает значительное снижение числа итераций при неизменных точностных характеристиках получаемой оценки.

**Ключевые слова:** *траекторные измерения; итерационный процесс; обработка измерений; начальное приближение; орбита типа «Молния».*

При обработке траекторных измерений с использованием метода наименьших квадратов (МНК), как известно, минимизируется выражение [1] вида

$$\Phi(\overline{X}) = \left(\overline{D} - \overline{Z}(\overline{X})\right)^T \cdot W \cdot \left(\overline{D} - \overline{Z}(\overline{X})\right), \quad (1)$$

где $\overline{D}$ — вектор измерений, W — весовая матрица ошибок измерений, а $\overline{Z}(\overline{X})$ — модель связи измеряемых параметров $\overline{Z}$ и оцениваемых $\overline{X}$.

Искомым значением вектора $\overline{X}$ является такое, при котором правая часть (1) достигает локального минимума.

Для уменьшения методических погрешностей оценивания модель измерений, описываемая векторной функцией $\overline{Z}(\overline{X})$, должна быть задана достаточно точно. Зачастую в некоторой окрестности начального приближения $\overline{X_0}$ функция $\overline{Z}(\overline{X})$ аппроксимируется линейной зависимостью, поскольку даже при незначительном усложнении функции аппроксимации минимизация правой части (1) существенно затрудняется. Так, при линейной аппроксимации искомый вектор $\overline{X}$ определяется [2] как

$$\overline{X} = \overline{X}_0 + (A^T \cdot W \cdot A)^{-1} \cdot A^T \cdot W \cdot \overline{\eta}, \quad (2)$$

где $A$ — матрица Якоби функции $\overline{Z}(\overline{X})$,

$\eta$ — вектор невязок измерений,

$W$ — весовая матрица ошибок измерений.

При использовании метода Ньютона [3], предполагающего учет вторых производных функции измерений, для поиска минимума (1) справедливо

$$\overline{X} = \overline{X}_0 - \left((B^T \cdot W \cdot \overline{\eta}) - A^T \cdot W \cdot A\right)^{-1} \cdot A^T \cdot W \cdot \overline{\eta}, \quad (3)$$

где B — массив матриц Гессе компонент функции $\overline{Z}(\overline{X})$.

Для учета нелинейных составляющих задача оценивания решается с использованием метода простой итерации. С другой стороны, его использование при высоких погрешностях начального приближения приводит к увеличению числа итераций или даже нарушению сходимости процесса решения.

В основу предложенной методики положен метод простой итерации, как наиболее пригодный для усовершенствований. Новизна методики заключается в структуре расчетов, проводимых на первой итерации, рассмотренной ниже.

Рассмотрим область отклонений начального приближения от истинного значения оцениваемого вектора, в которой целесообразна линейная аппроксимация $\overline{Z}(\overline{X})$.

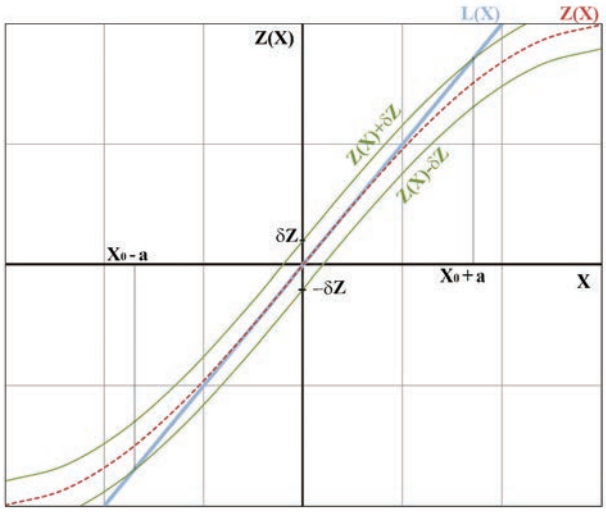



**Рис. 1.** Область линейности скалярной функции

На рис. 1 проиллюстрирован случай, когда Z(X) является скалярной функцией скалярного аргумента. Эту функцию можно аппроксимировать линейной зависимостью в некоторой области $[X_0 - a; X_0 + a]$.

Размеры данной области зависят от характера Z(X) и допуска δZ, связанного с погрешностью измерений — при снижении измерительных погрешностей, а также при усилении нелинейного характера Z(X) величина *a*, как видно из рисунка, будет уменьшаться.

Если начальное приближение имеет погрешность выше этой величины, пренебрежение нелинейной составляющей Z(X) может привести к снижению точности оценки либо к увеличению числа итераций.

Поскольку при обработке траекторных измерений функция $\overline{Z}(\overline{X})$ является векторной, каждая из её компонент имеет различный характер нелинейности. Так, если данные получены в различных измерительных каналах, то и характеристики измерительных погрешностей будут различны. Таким образом, размер области, в которой зависимость $Z_i(\overline{X})$ можно принимать линейной, для различных компонент вектора измерений будет различным.

Назовем «областью линейности» M векторной функции измерений $\overline{Z}(\overline{X})$ такую область в пространстве оцениваемых параметров, включающую начальное приближение, что для любого значения вектора $\overline{X}$, принадлежащего данной области, разница между линейной аппроксимацией функции $\overline{Z}(\overline{X})$ и её истинным значением не превышает установленного значения допуска $\delta\overline{Z}$:

$$\forall\overline{X} \in M \Rightarrow \forall i \in [1;n] \Rightarrow \left|Z_i(\overline{X}) - [Z_i(\overline{X}_0) + TZ_i(\overline{X}_0)]\right| \le \delta Z_i, \quad (4)$$

$$T = \sum_{j=1}^{m}(X_j - X_{0j}) \cdot \frac{\partial}{\partial X_j}, \quad (5)$$

где T — оператор вида

n — размерность вектора измерений,

m — размерность оцениваемого вектора.

Для снижения влияния нелинейного характера отдельных компонент функции $\overline{Z}(\overline{X})$ стоит разбить измерения на группы и проводить их обработку по нарастающей выборке [3]. Тогда измерения будут включаться в расчеты поэтапно, а на каждом этапе будет обрабатываться группа измерений с наибольшими размерами области линейности. В этом случае погрешность начального приближения, используемого для определения параметров линеаризованной модели измерений с небольшой областью линейности, будет меньше.

Если в обработке участвуют измерения, поступающие из различных каналов, один из вариантов разбиения измерений на поочередно обрабатываемые группы — так, чтобы каждая из групп соответствовала отдельному измерительному каналу. Например, если имеются измерения радиальной скорости КА относительно измерительных средств (Ḋ), углового положения КА (α, β) и разности дальностей от КА до двух измерительных средств (Δ*D*), то в этом случае вектор $\overline{Z}(\overline{X})$ можно представить в следующем виде:

$$\overline{Z}(\overline{X}) = \begin{pmatrix} \overline{Z_{\dot{D}}}(\overline{X}) \\ \overline{Z_{\alpha,\beta}}(\overline{X}) \\ \overline{Z_{\Delta D}}(\overline{X}) \end{pmatrix}. \quad (6)$$

Рассмотрим количественные характеристики, служащие критерием для выбора порядка обработки измерений. Предположим, что порядок обработки целесообразно выбирать исходя из размера области линейности, построенной для каждой группы измерений.

Чтобы получить представление об искомых областях, рассмотрим уравнения поверхностей, ограничивающей область $M_i$ для каждого значения i. Тогда отклонение линеаризованной функции $L_i(\overline{X})$ от истинного значения $Z_i(\overline{X})$ совпадает с допуском $\delta Z_i$:

$$\left|Z_i(\overline{X}) - L_i(\overline{X})\right| = \delta Z_i. \quad (7)$$

Рассматриваемый критерий строится в предположении, что при разложении $Z_i(\overline{X})$ в ряд Тейлора можно ограничиться первыми тремя членами [5]

$$Z_i(\overline{X}) = Z_i(\overline{X}_0) + TZ_i(\overline{X}_0) + \frac{T^2 Z_i(\overline{X}_0)}{2}. \quad (8)$$

Если в качестве порогового значения $\delta Z_i$ принять СКО погрешности i-го измерительного канала, умноженное на некоторый коэффициент k, то уравнение поверхности, ограничивающей область линейности соответствующей функции, примет вид:

$$\left|(\overline{X} - \overline{X}_0)^T F_i (\overline{X} - \overline{X}_0)\right| = k\sigma_i. \quad (9)$$

где $F_i$ — матрица Гессе, содержащая вторые производные компоненты измерений $Z_i$ по компонентам вектора $\overline{X}$, взятые в точке $X_0$.

Уравнение (9) описывает [4] семейство поверхностей второго порядка. Примем, что законы распределения ошибок различных измерений одинаковы. Тогда величина k для всех значений *i* является постоянной, а ее значение не оказывает влияния на выбор порядка обработки. В дальнейшем величина *k* была принята равной единице и исключена из расчетных зависимостей, что не меняет общности последующих заключений.

Область $M_i$ описывается неравенством

$$\left|(\overline{X} - \overline{X}_0)^T F_i (\overline{X} - \overline{X}_0)\right| \le \sigma_i, \quad (10)$$

а искомая область линейности группы измерений является пересечением областей $M_i$ для всех значений i, которые соответствуют данной группе.

Искомая область имеет сложную форму, а точное определение её размера весьма трудоемко. Наиболее практичным для реализации способом оценить её размер является использование метода прямого перебора. Также можно аппроксимировать данную область фигурой, форма которой удобна для подобных расчетов.

В данной работе рассмотрена аппроксимация каждой области $M_i$ m-мерным брусом, грани которого пересекают координатные оси в точках пересечения поверхности (9) с соответствующими осями. При пересечении большого числа таких областей возможно достижение приемлемой точности аппроксимации.

В таблице 1 приведено сравнение результатов расчетов методом прямого перебора и предложенного выше способа аппроксимации. Величина *L* — некоторая линейная характеристика размера областей линейности, полученная методом прямого перебора. Величина *D* — половина длины диагонали аппроксимирующих данные области брусов. Все расчеты проводились для трехмерного пространства без учета скоростных составляющих. Таким образом, размерность *m* рассматриваемой задачи равна трем.

Расчеты проводились по следующим исходным данным [6]:

— КА движется по орбите типа «Молния»;

— измерения содержат информацию о разности дальностей от КА до измерительных средств (РДК-измерения), а также об угловом положении и радиальной скорости КА относительно каждого из них;

— ошибки измерений некоррелированы между собой и распределены по нормальному закону с нулевым математическим ожиданием и известной дисперсией;

— измерения проводятся во время прохождения КА рабочего участка (РУ) орбиты продолжительностью 7 часов, симметрично расположенного по времени относительно апогея текущего витка.

Рассмотрены два варианта планирования измерений: на четырех последовательных РУ по 4 измерения на каждом и на двух РУ с перерывом в одни сутки по два измерения на каждом. Общее число измерений составило 16 и 4 соответственно.

Таблица 1. Сравнение методов аппроксимации брусоми прямого перебора

| | | D, км | L, км | Отличие, % |
|---|---|---|---|---|
| 4 РУ по 4 измерения | α,β | 181.0 | 178.8 | 0.2 |
| | Ḋ | 64.2 | 65.1 | 1.9 |
| | ΔD | 46.8 | 42.8 | 8.5 |
| 2 РУ по 2 измерения | α,β | 205.9 | 197.5 | 4.1 |
| | Ḋ | 70.3 | 80.7 | 14.8 |
| | ΔD | 52.9 | 58.2 | 10.0 |

Из приведенных данных видно, что при увеличении числа измерений точность аппроксимации повышается, однако и при небольшом их числе точность достаточна для оценки соотношения размеров искомых областей, что и требуется для использования предлагаемого критерия. Визуализация рассматриваемых областей, полученная методом прямого перебора, приведена на рис. 2 и 3.

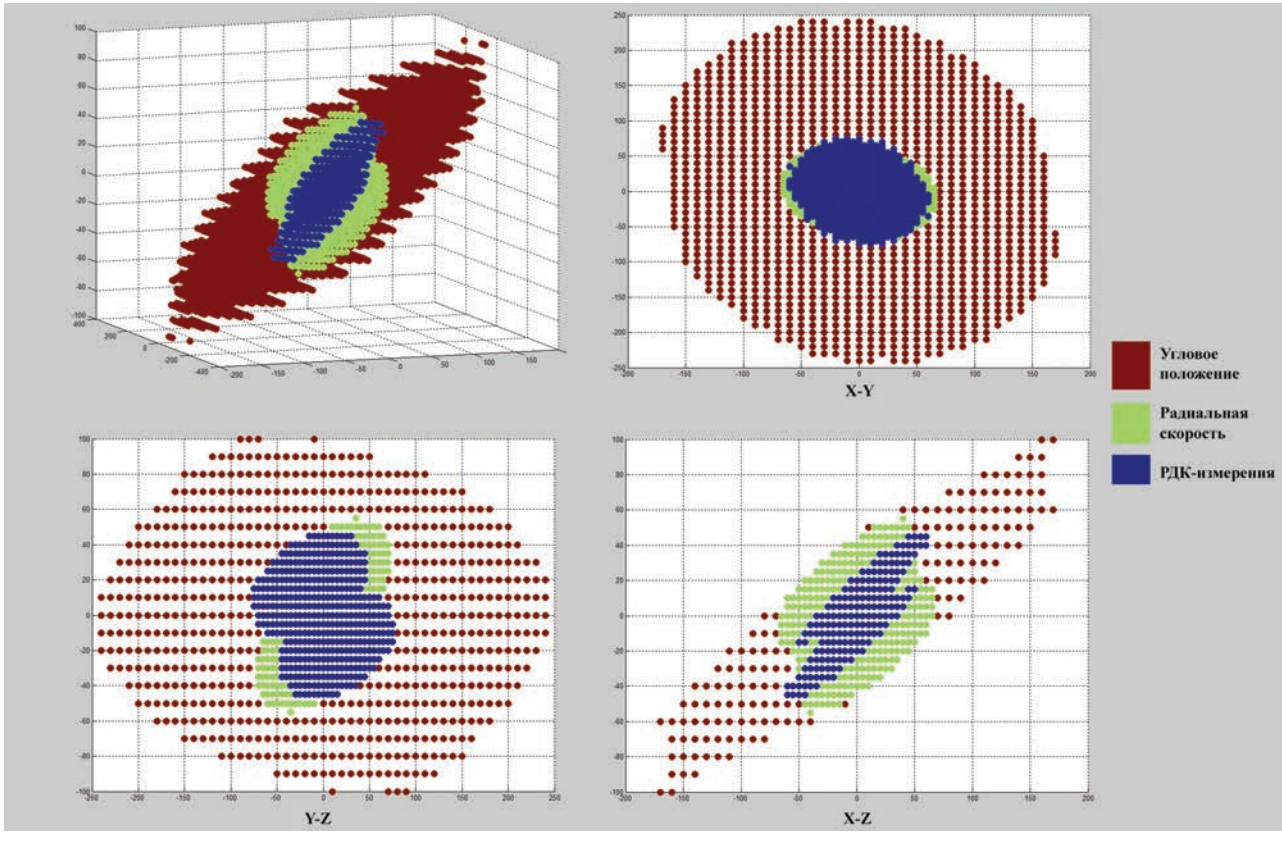



**Рис. 2.** Построенные области линейности для измерений на двух РУ

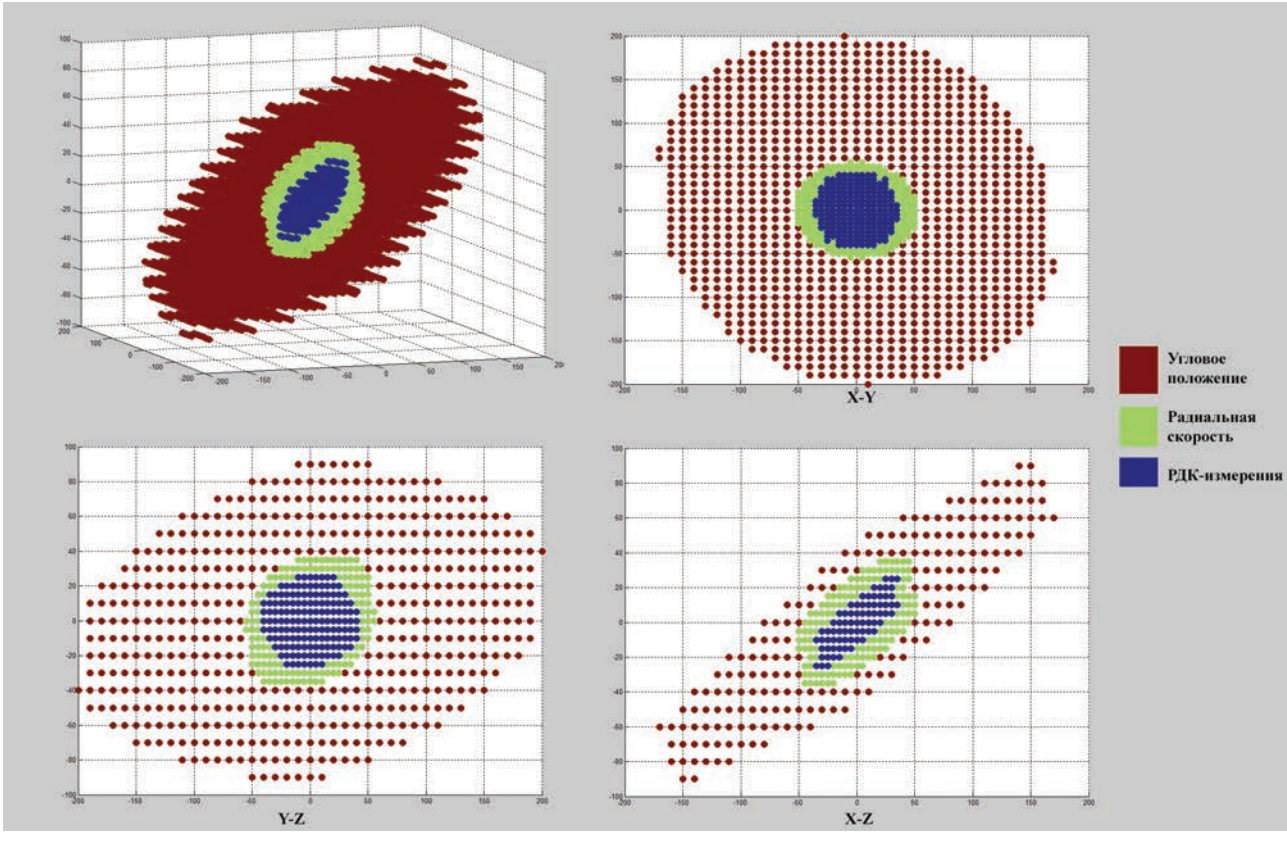



**Рис. 3.** Построенные области линейности для измерений на четырех РУ

Видно также, что, исходя из предложенного критерия, рекомендуемый порядок включения измерений в обработку имеет вид:

угломерные измерения;

радиально-скоростные измерения;

разностно-дальномерные измерения.

Рассмотрим результаты использования предложенного критерия при обработке измерений. Выдвинутые на основе теории предположения о рекомендованном порядке были проверены посредством статистического моделирования работы алгоритма оценивания с использованием аналогичных входных данных. Моделируемое СКО начального приближения орбиты КА составило 370 км по положению. Выборка, полученная при моделировании, составила 1000 реализаций.

На рис. 4 и 5 представлены экспериментально полученные графики зависимости от $i$ величины $P$, определяемой как

$$P = P[|\delta X| > i\sigma_{\delta X}], \tag{11}$$

где $\delta X$ — погрешность оценки положения КА, полученной на первой итерации,

$\sigma_{\delta X}$ — СКО погрешности оценки положения КА.

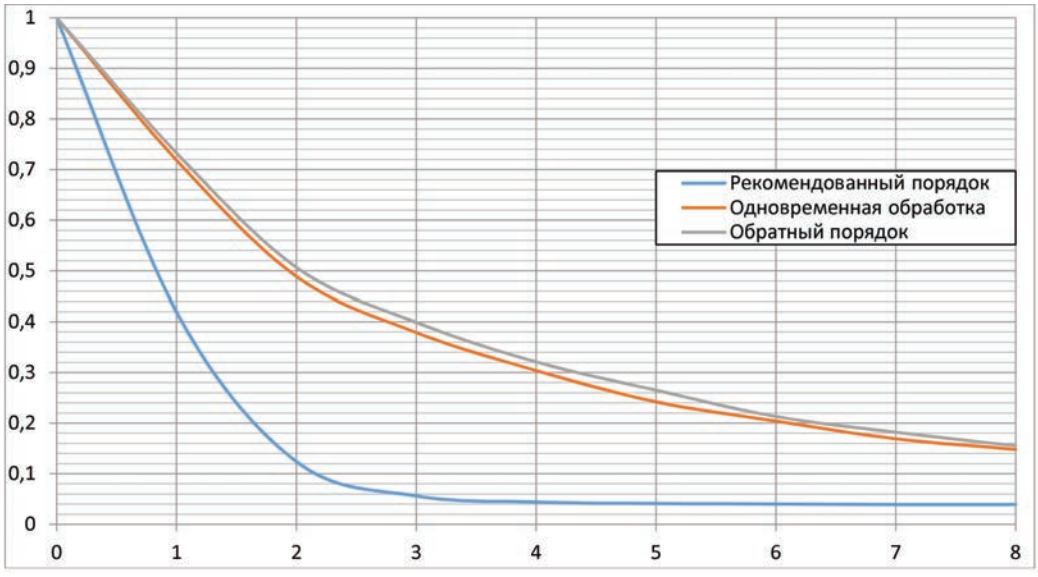



**Рис. 4.** Распределение ошибок оценки положениядля измерений на двух РУ

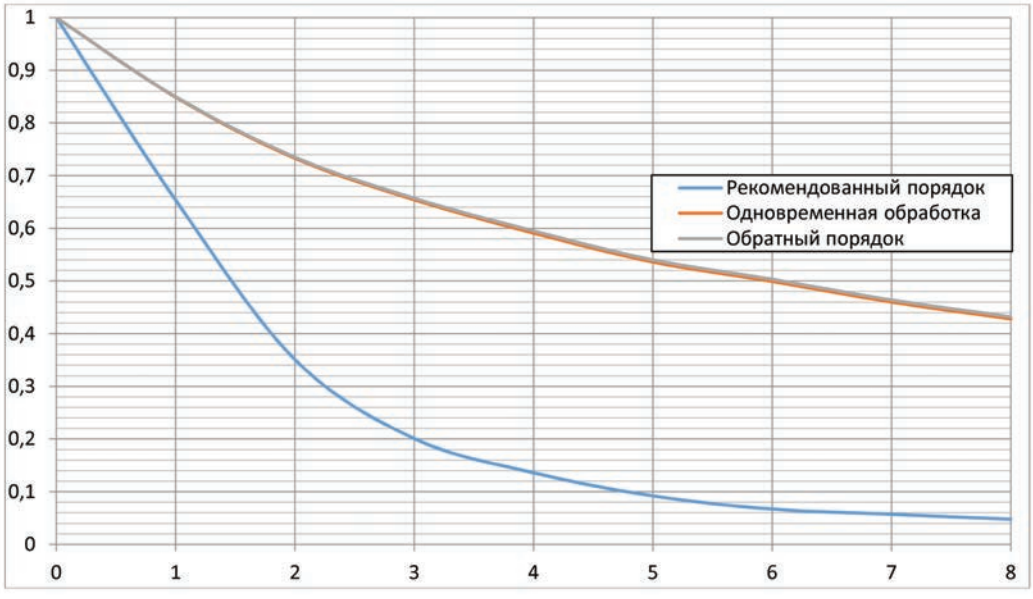



**Рис. 5.** Распределение ошибок оценки положения для измерений на четырех РУ

Данные графики получены при единовременном, а также раздельном учете измерений в различной последовательности. По оси абсцисс отложена величина *i*. По оси ординат — вероятность *P* попадания оценки, отнесенной к её СКО, в интервал (*i*; +∞).

Синяя кривая, соответствующая рекомендованному порядку обработки, имеет наиболее выраженный спад, что говорит о низкой вероятности получения больших погрешностей оценки. Зеленая и красная кривые, соответствующие обработке в порядке, обратном рекомендованному, и одновременной обработке измерений, имеют худшие показатели, схожие между собой.

Из графиков видно, что для зеленой и красной кривых имеет место высокая вероятность больших погрешностей оценивания на первой итерации. В частности, при обработке измерений на двух РУ вероятность того, что отклонение оценки от истинного значения превысит утроенное СКО, близка к значению 0.4, а при наличии измерений на четырех РУ — к значению 0.65. В то же время при обработке измерений в рекомендованном порядке данная вероятность не превышает 0.05 для измерений на двух РУ и 0.2 — на четырех.

При этом общее число итераций за счет использования рекомендованного порядка обработки измерений сократилось в 70% реализаций.

**Выводы**

Использование предложенного критерия выбора последовательности обработки измерений позволяет:

1. Минимизировать влияние погрешностей начального приближения орбитального вектора на результаты оценивания.
2. Улучшить вероятностные характеристики оценок, получаемых на первой итерации.

В частности, вероятность того, что погрешность оценки, полученной на первой итерации, превысит порог в 3σ, для измерений на двух РУ по сравнению с одновременной обработкой снизилась почти на порядок, а для измерений на четырех РУ — более, чем в три раза.

3. Использование разработанной методики обработки траекторных измерений при формировании начального приближения приводит к ускорению сходимости решения задачи оценивания. При проведении расчетов по использованным исходным данным ускорение сходимости наблюдалось в 70% случаев.

**Список литературы**

1. *Эльясберг П. Е.* Определение движения по результатам измерения. М.: Наука, 1976. 416 с.
2. *Жданюк Б. Ф.* Основы статистической обработки траекторных измерений. М., Советское радио, 1978, 384 с.
3. *Самарский А. А.*, *Гулин А. В.* Численные методы. М.: Наука, 1989. 432 с.
4. *Корн Г.*, *Корн Т.* Справочник по математике для научных работников и инженеров. М.: Наука, 1974, 832 с.
5. *Зорич В. А.* Математический анализ. Ч. 2. М.: Наука, 1981. 544 с.
6. *Чернявский Г. М.*, *Бартенев В. А.* Орбиты спутников связи. М.: Связь, 1978. 240 с.

## ACCELERATION OF CONVERGENCE OF PROCESS OF PROCESSING TRAJECTORY MEASUREMENTS OF SPACECRAFTS IN TYPE "MOLNIYA" ORBITS AT HIGH ERRORS OF INITIAL APPROACH

**Doronkin Aleksey Valeryevich**,
Moscow, Russia, bj13@yandex.ru

**Abstract**

A procedure of different-precision spacecraft trajectory measurements processing, based on the analysis of poly-dimensional relation measurand to evaluated parameters function linearity characteristics was offered. Statistical modeling shows that proposed procedure increases accuracy of initial approximation used by spacecraft orbital parameters evaluation iterative process. It provides number of iteration to be substantially smaller without estimate accuracy changes in the same time.

**Keywords:** trajectory measurements; iterative process; measurement processing; initial approximation; Molniya orbit.

**References**

1. Elyasberg P. E. Opredeleniye dvizheniya po rezultatam izmereniya [Movement definition by results of measurement]. Moscow, Nauka, 1976. 416 p. (In Russian)
2. Zhdanyuk B. F. Osnovy statisticheskoy obrabotki traektornykh izmereniy [Bases of statistical processing of trayektorny measurements]. Moscow, Sovetskoye radio, 1978. 384 p. (In Russian).
3. Samarskiy A.A, Gulin A. V. Chislennye metody [Numerical methods]. Moscow, Nauka, 1989. 432 p. (In Russian)
4. Korn G., Korn T. Spravochnik po matematike dlya nauchnykh rabotnikov i inzhenerov [Справочник по математике для научных работников и инженеров]. Moscow, Nauka, 1974. 832 p. (In Russian)
5. Zorich V. A. Matematicheskiy analiz [Mathematical analysis]. Pt.2. Moscow, Nauka, 1981. 544 p. (In Russian)
6. Chernyavskiy G. M., Bartenev V. A. Orbity sputnikov svyazi [Orbits of communication satellites]. Moscow, Svyaz, 1978. 240 p. (In Russian)

**Information about author:**
Doronkin A. V., engineer-researcher of 1 category "Cometa" corporation.

РОССИЙСКАЯ НЕДЕЛЯ
ВЫСОКИХ ТЕХНОЛОГИЙ

# СВЯЗЬ

## Информационные и коммуникационные технологии

## 25–28 апреля 2017

В НОВЫЕ СРОКИ

29-я международная выставка

Организатор:

ЭКСПОЦЕНТР МОСКВА

При поддержке:

- Государственной Думы Федерального Собрания РФ
- Министерства связи и массовых коммуникаций РФ
- Министерства промышленности и торговли РФ
- Федерального агентства связи (Россвязь)
- Российской ассоциации электронных коммуникаций (РАЭК)

Под патронатом Торгово-промышленной палаты РФ

Россия, Москва, ЦВК «Экспоцентр»

**www.sviaz-expo.ru**

Реклама 12+

## ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

Предоставляемая для публикации статья 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 научно-теоретический уровень публикуемого материала.

1. Статья подготавливается в редакторе MS Word.
2. Формульные выражения выполняются в редакторе Math Type. Также в отдельной папке должны содержаться экспортированные изображения формул в формате TIFF (качество изображений не менее 300 dpi). Названия файлов должны соответствовать номерам формул в статье (Например: Формула 1.tif).
3. Объём статьи без аннотации – от 10 до 20 тыс. знаков. Рисунки и таблицы в объеме статьи не учитываются.
4. Объем аннотации 250-300 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.
5. Ключевые слова (не менее пяти), разделенных точкой с запятой.
6. Фамилия, имя, отчество, ученая степень, звание, должность и полное название организации - места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.
7. Список литературы не менее пяти наименований, для статей - с указанием страниц, для книг – с указанием общего числа страниц в книге, для интернет-сайта – с указанием даты обращения. 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 7.05-2008. Образец оформления списка литературы размещен на сайте журнала.
8. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается.
9. На английском языке предоставляется: название статьи, фамилия, имя, отчество, город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.
В конце размещается полная информация об авторах (возможно размещение кратких автобиографий): фамилия, инициалы, должность, ученая степень, ученое звание, место работы (организация) и другие данные с надписью (Information about authors).
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.
10. Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, ключевые слова, аннотация, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями рисунков и формул в формате TIFF, по требованиям указанным в п.2. Тексты в рисунках должны быть читаемы.
11. 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
Редакция принимает к публикации статьи на английском языке.
**Внимание!** Редакция оставляет за собой право отклонить представленные материалы, оформленные не по указанным правилам.

## MANUSCRIPT REQUIREMENTS

**Format**

1. All files should be submitted as a Word document.
2. Articles should be between 15000 and 20000 characters (incl. spaces).
3. Article Title to be submitted in native language and English. A title of not more than eight words should be provided.

**Author Details** (in English and native language)

Details should be supplied on the Article Title Page including:

* Full name of each author
* Position, rank, academic degree
* Affiliation of each author, at the time the research was completed
* Full postal address of the affiliation
* E-mail address of each author
* Structured Abstract (in English and native language)
* Abstract should be: informative (no general words), original, relevant (reflects your papers key content and research findings); structured (follows the logics of results presentation in the paper), concise (between 250 and 300 words).
* Purpose (mandatory)
* Design/methodology/approach (mandatory)
* Findings (mandatory)
* Research limitations/implications (if applicable)
* Practical implications (if applicable)
* Social implications (if applicable)
* Originality/value (mandatory)

It is appropriate to describe the research methods/methodology if they are original or of interest for this particular research. For papers concerned with experimental work describe your data sources and data procession technique. Describe your results as precisely and informatively as possible. Include your key theoretical and experimental results, factual information, revealed interconnections and patterns. Give special priority in your abstract to new results and long-term impact data, important discoveries and verified findings that contradict previous theories as well as data that you think have practical value.

Conclusions could be associated with recommendations, estimates, suggestions, hypotheses described in the paper.

Information contained in the title should not be dublicated in the abstract. Try to avoid unnecessary introductory phrases (e.g. the author of the paper considers).

Use the language typical of research and technical documents to compile your abstract and avoid complex grammatical constructions. The text of the abstract should include key words of the paper.

**Keywords** (in English and native language)

Please provide up to 5 keywords on the Article Title Page, which encapsulate the principal topics of the paper.

**Figures**

All figures should be of high quality, legible and numbered consecutively with arabic numerals. All figures (charts, diagrams, line drawings, web pages/screenshots, and photographic images) should be submitted in electronic form preferably in color as separate files, that match the following parameters: TIFF format (quality of figures not less than 300 dpi).

**References**

References to other publications must be in Harvard style and carefully checked for completeness, accuracy and consistency.