

SCCS



**Системы управления,
связи и безопасности**

**Systems of Control,
Communication and
Security**

ISSN 2410-9916
<http://sccs.intelgr.com>

№3 2015

ООО «Корпорация «Интел Групп»

Системы управления, связи и безопасности

Периодическое электронное издание
комплексного распространения

Научный журнал

Издается с апреля 2015 года
Выходит один раз в квартал

№ 3
III квартал 2015 г.

Журнал «Системы управления, связи и безопасности» является научным рецензируемым периодическим электронным изданием. Цель журнала – максимально полное, оперативное и открытое информирование научной общественности об основных результатах научно-исследовательских работ в области теории управления, теории связи, теории безопасности, а также о новых тенденциях развития технологий соответствующих прикладных областей.

Периодичность выхода журнала – четыре номера в год.

Журнал «Системы управления, связи и безопасности» публикует только статьи, которые соответствуют основным тематическим разделам журнала:

1. Анализ новых технологий и перспектив развития систем управления, связи и безопасности.
2. Системы управления.
3. Интеллектуальные информационные системы.
4. Робототехнические системы.
5. Вычислительные системы.
6. Информационные процессы и технологии. Сбор, хранение и обработка информации.
7. Информационная безопасность.
8. Передача, прием и обработка сигналов. Радиоэлектронный мониторинг.
9. Системы связи и телекоммуникации.
10. Системы обеспечения безопасности.
11. Моделирование сложных организационно-технических систем.
12. Объекты интеллектуальной собственности и инновационные технологии в области управления, связи и безопасности.

Публикация в журнале является научным печатным трудом.

Журнал доступен по адресу <http://sccs.intelgr.com>.

Содержание

Юдицкий С.А. ВОСПОМИНАНИЯ ВЕТЕРАНА ИНЖЕНЕРНОЙ НАУКИ: ПНЕВМОАВТОМАТИКА. ЛОГИЧЕСКОЕ УПРАВЛЕНИЕ ДИСКРЕТНЫМИ ПРОЦЕССАМИ. МОДЕЛИРОВАНИЕ СЛОЖНЫХ ДИСКРЕТНЫХ СИСТЕМ	1
Абазина Е.С. МЕТОД КОДОВОГО УПЛОТНЕНИЯ СКРЫТОГО КАНАЛА ПРИ ПЕРЕДАЧЕ ВИДЕОДАНЫХ	16
Юдицкий С.А. “ДОРОЖНЫЕ КАРТЫ” С ПРИНЯТИЕМ РЕШЕНИЙ НА ГИБРИДНЫХ ИНДИКАТОРНЫХ СЕТЯХ	43
Михайлов Р.Л. МОДЕЛИ И АЛГОРИТМЫ МАРШРУТИЗАЦИИ В ТРАНСПОРТНОЙ НАЗЕМНО-КОСМИЧЕСКОЙ СЕТИ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ	52
Алексеев А.П. УЯЗВИМОСТИ АЛГОРИТМА ВЫЧИСЛЕНИЯ СЕКРЕТНОГО КЛЮЧА В КРИПТОСИСТЕМЕ RSA	83
Аганесов А.В. АНАЛИЗ КАЧЕСТВА ОБСЛУЖИВАНИЯ В ВОЗДУШНО-КОСМИЧЕСКОЙ СЕТИ СВЯЗИ НА ОСНОВЕ ИЕРАРХИЧЕСКОГО И ДЕЦЕНТРАЛИЗОВАННОГО ПРИНЦИПОВ РЕТРАНСЛЯЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ	92
Макаренко С.И. ДИНАМИЧЕСКАЯ МОДЕЛЬ СИСТЕМЫ СВЯЗИ В УСЛОВИЯХ ФУНКЦИОНАЛЬНО-РАЗНОУРОВНЕВОГО ИНФОРМАЦИОННОГО КОНФЛИКТА НАБЛЮДЕНИЯ И ПОДАВЛЕНИЯ	122
Алексеев А.П., Дикарева К.Н., Макаров М.И. АНАЛИЗ БЫСТРОДЕЙСТВИЯ АЛГОРИТМОВ ВЫЧИСЛЕНИЯ СЕКРЕТНОГО КЛЮЧА В АСИММЕТРИЧНОЙ КРИПТОСИСТЕМЕ RSA	186
Воронин Ю.Ф., Камаев В.А. ТРЕНАЖЕР ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБУЧЕНИЯ СТУДЕНТОВ ВУЗОВ И ТЕХНОЛОГОВ ЛИТЕЙНЫХ СПЕЦИАЛЬНОСТЕЙ	210

Архив выпусков журнала доступен по адресу <http://sccs.intelgr.com/arch.html>.

Главный редактор С.И. Макаренко

Редакционная коллегия:

А.В. Баженов, П.А. Будко, В.В. Борисов, Е.В. Гречишников, В.М. Коровин (тех. ред.), Ю.А. Кропотов, В.И. Левин, Г.И. Линец, А.С. Марков, Р.Л. Михайлов, Е.А. Новиков, С.С. Семенов

Правила для авторов

Материалы, представляемые в редакцию

1. Файл со статьей, оформленной по образцу (<http://sccs.intelgr.com/download/article.doc>).
2. Сканированную копию экспертного заключения об отсутствии в статье материалов, запрещенных к открытому опубликованию, в файле формата jpg, 300 dpi, в цвете.
3. По отдельному запросу редакции файлы с рисунками, выполненные в векторном формате vsd, wmf, emf, или в растровых форматах png или jpg.
4. Указание на необходимость оформления авторских справок о публикации, их количестве и порядке отправки авторам.
5. Авторы могут подготовить краткое сообщение рецензенту, дополнительно поясняющее отдельные элементы работы, их суть и новизну, рамки исследования, связь своей работы с имеющимися публикациями в предметной области. Данное сообщение необязательно, но, при его наличии, оно будет передано рецензенту вместе со статьей.

Порядок рецензирования и принятия статьи к публикации

1. Авторский коллектив представляет в редакцию статью и сопроводительные материалы на адрес sccs@intelgr.com.
2. Редакция осуществляет проверку материалов на предмет соответствия требованиям к оформлению и представлению результатов. При необходимости технической правки статьи авторы уведомляются об этом.
3. Если замечаний по оформлению статьи нет, она проверяется в сервисах, выявляющих плагиат, и с результатами проверки передается на рецензирование. Редакция уведомляет авторов о передаче статьи на рецензирование.
4. Порядок проверки на плагиат и выбор сервиса для проверки определяется редакцией самостоятельно. Для проверки на плагиат редакцией используются Интернет-сервисы Антиплагиат, TEXT, Content-watch, а также программы Etxt и Advego Plagiatus.
5. В случае положительного решения рецензентов о возможности публикации статьи авторы уведомляются об этом. В случае несовпадения мнений рецензентов о возможности публикации статьи, она передается на повторное рецензирование или рассматривается редакционной коллегией журнала, о чем уведомляется авторский коллектив. В случае решения рецензентов или редакционной коллегии журнала о невозможности публикации статьи авторы получают мотивированный отказ.
6. По решению рецензентов или редакционной коллегии статья может быть принята к публикации, но с доработками. В этом случае авторы должны в короткий срок переработать статью в соответствии с замечаниями рецензентов, либо дать мотивированный ответ по замечаниям. Если доработка статьи потребует значительного времени, авторы должны уведомить об этом редакцию.
7. После принятия статьи к публикации, авторы оплачивают редакционные расходы, связанные с публикацией статьи.
8. После оплаты редакционных расходов статья размещается в очередном номере журнала на сайте издательства. Авторы уведомляются о публикации их статьи по электронной почте.
9. После формирования очередного номера журнала данные об опубликованных в нем статьях в течение трех месяцев передаются в наукометрические базы учета научных публикаций.

Пример оформления статьи доступен по адресу <http://sccs.intelgr.com/download/article.doc>

1. Статья представляется в формате Word 97/2000/XP с расширением **doc**.
2. Рекомендуемый объем статьи – **до 50 страниц**. Объем может быть увеличен, если этого требует логика изложения материала.
3. Размер страницы – А4. Все поля (верхнее, нижнее, правое и левое) по 2 см.
4. Текст статьи набирается шрифтом Times New Roman, размер шрифта 14 pt, одинарный междустрочный интервал, абзацный отступ 1,25 см, отступы между абзацами отсутствуют. В основном тексте допускаются выделения курсивом. Латинские буквы для обозначения переменных набираются курсивом; греческие, русские буквы, функции – прямым шрифтом. Цифровые индексы в обозначениях набираются прямым шрифтом.
5. Статья должна начинаться с индекса УДК, выровненного по левому краю. После индекса УДК следует пропуск строки.
6. Название статьи должно точно и однозначно характеризовать содержание статьи. Название статьи – полужирным шрифтом, выравнивание по центру без абзацного отступа. **Название писать строчными (маленькими) буквами**, используя заглавные буквы только там, где это необходимо (в начале первого слова, в названиях, именах собственных, сокращениях и т.п.). Не рекомендуется использовать в названии сокращения, кроме общепринятых в соответствующей предметной области. Точка после заглавия НЕ ставится. После названия статьи следует пропуск строки.
7. Фамилии и инициалы авторов указываются через запятую в последовательности, соответствующей личному вкладу в написание статьи. Фамилии авторов выравниваются по центру страницы без абзацного отступа. Между фамилией и первым инициалом, а также между инициалами ставится неразрывный пробел (Ctrl+Shift+пробел). После фамилий авторов следует пропуск строки.
8. Аннотация выполняется на русском и английском языке в соответствии с [рекомендациями по написанию авторского резюме](#). Оформление аннотации: размер шрифта **11pt**, курсив, абзацный отступ 1,25 см. Заголовки отдельных элементов в структуре аннотации выделяются жирным шрифтом. После аннотации следует пропуск строки.
9. Ключевые слова оформляются так же, как и аннотация, и должны содержать основные понятия и термины, употребляемые в статье. Ключевые слова должны формулироваться таким образом, чтобы при семантическом поиске по ним можно было найти данную статью потенциально заинтересованным ученым. После абзаца с ключевыми словами следует пропуск строки.
10. Для структуризации статьи рекомендуется основной текст разделить по частям, имеющим условные подзаголовки «Введение», «Постановка задачи» («Формализация задачи»), «Модель...» («Методика...», «Метод...»), «Результаты моделирования» («Обоснование...»), «Выводы». Подзаголовки выполняются полужирным шрифтом и выравниваются по центру страницы без абзацного отступа. Перед подзаголовками следует пропуск одной строки.
11. Таблицы выравниваются по центру без абзацного отступа. Текст внутри таблиц может выполняться шрифтом от 10pt до 14pt, в зависимости от степени информационной загрузки ячеек таблиц. Таблицы нумеруются по порядку упоминания, а их названия оформляются в виде «Таблица 1 – Название таблицы» и выравниваются по центру без абзацного отступа. Если таблица выполняется на нескольких страницах, необходимо выставлять признак заголовка для первой строки с наименованиями столбцов, либо дублировать первую строку с наименованиями на следующей странице.
12. Рисунки выполняются в виде внедренных объектов векторной графики, выполненных в формате MS Visio (**vsd**) или в форматах метафайлов Windows (**wmf** или **emf**). В случае невозможности представления рисунков в векторном виде, рисунки выполняются в растровых форматах **jpg** или **png**. Нумерация рисунков последовательная по мере упоминания в статье в виде «Рис. 1. Название рисунка». Номер и название рисунка выравниваются по центру без абзацного отступа. До рисунка и после его названия вставляется пропуск строки. Допускается выполнение рисунков, расположенных параллельно друг другу на одном горизонтальном уровне. В этом случае рисунки и их названия помещаются в таблицу с прозрачными границами.

13. Формулы выполняются в редакторе формул MathType или Microsoft Equation 3.0. Формулы могут быть набраны в основном тексте со вставкой специальных математических символов через меню «Вставка-Символы». **Запрещается набирать формулы во встроенном редакторе формул Microsoft Office 2007 и выше.** Основной шрифт формул набираемых в MathType и Microsoft Equation 3.0, 12 pt или 14 pt. Формулы выравниваются по левому краю с абзацным отступом 2,5 см. При необходимости переноса формул используется общепринятая математическая запись переноса. Формулы, на которые есть ссылки в тексте статьи, должны быть пронумерованы. Номер формулы проставляется с правого края страницы. При оформлении формул, не следует вставлять дополнительные пропуски строки до и после формул.
14. Для облегчения редактирования статьи просим выделять **желтым маркером** номера формул, номера рисунков, ссылки на литературу, ссылки на формулы и рисунки в основном тексте статьи.
15. В конце статьи, по желанию авторов, могут быть приведены высказывания благодарности за помощь в исследованиях, сведения о грантах, НИРах и ОКРах, в рамках которых выполнялась работа, а также сведения об источниках финансирования исследований. Также в конце статьи авторами могут быть представлены приложения, где содержатся листинги программ, на основе которых выполнялось моделирование, различные объемные таблицы и графики, а также другие элементы, которые с одной стороны являются неотъемлемой частью исследования, а с другой - загромождают текст статьи.
16. Список используемых источников оформляется в соответствии с **требованиями к оформлению библиографических ссылок нашего журнала** после подзаголовка «Литература», который выполняется полужирным шрифтом, выравниваются по центру страницы без абзацного отступа. Нумерация ссылок определяется порядком их упоминания в статье. При формировании списка литературы не следует использовать функцию автоматического формирования нумерованного списка. После подзаголовка «Reference» литература дублируется на английском языке. При оформлении списка литературы и его перевода редакция настоятельно просит авторов пользоваться и соблюдать требования и **рекомендации по оформлению списка литературы и его переводу на английский язык**. После списка литературы и Reference следует пропуск строки.
17. После списка Reference указывается дата первого представления статьи в редакцию. Данный абзац выделяется полужирным шрифтом, выравнивание по правому краю страницы.
18. В конце статьи указывается информация об авторах. Данные сведения для каждого соавтора обязательно должны содержать: фамилию, имя, отчество полностью, научную степень, научное звание, должность и полное наименование организации, телефон и e-mail.
19. Статья завершается текстовым блоком, дублирующим название статьи, фамилии и инициалы авторов, аннотацию статьи и ключевые слова на английском языке. Данный текстовый блок начинается с новой страницы и его элементы оформляются так же, как соответствующие элементы на русском языке в начале статьи.

Требования к оформлению блока, содержащего сведения об авторах. Нижеуказанные сведения приводятся по каждому автору отдельно.

1. Фамилия, Имя, Отчество на русском языке.
2. Научная степень и научное звание (если есть) на русском языке.
3. Место работы с указанием страны и города на русском языке. Указывается официальное название, желательно из устава, в именительном падеже. Так как базы цитирования (например, РИНЦ) «привязывают» статью к определенному автору в определенной организации, то неверное указание места работы может привести к тому, что Ваша статья может отсутствовать в списке Ваших публикаций в базах цитирования, а также в списке публикаций сотрудников Вашей организации.
4. Должность на русском языке.
5. Область научных интересов – на русском языке.
6. Адрес электронной почты. Убедительная просьба указывать существующий и действующий адрес электронной почты для КАЖДОГО соавтора.
7. Корреспондентский почтовый адрес (с индексом) для контактов с авторами статьи. Данный адрес можно указать один на всех авторов. Можно указать как рабочий (предпочтительно), так и домашний (по желанию) адрес. Обратите внимание на то, что эта информация будет опубликована в открытом доступе.
8. Телефон для связи.

1. Фамилия, Имя, Отчество на английском языке.
2. Научная степень и научное звание (если есть) на английском языке. При затруднениях, связанных с переводом, просим воспользоваться [рекомендациями по переводу должности, ученой степени и ученого звания](#).
3. Международное название места работы с указанием страны и города на английском языке (желательно, в соответствии с уставом). Переводить по буквам аббревиатуры в названии НЕ НУЖНО. Редакция просит Вас воздержаться от использования аббревиатур и сокращений, кроме аббревиатур, указывающих на организационно-правовую форму места работы автора (ФГБОУ, ООО, ОАО и т. п.).
4. Должность на английском языке. При затруднениях, связанных с переводом, просим воспользоваться [рекомендациями по переводу должности, ученой степени и ученого звания](#).
5. Область научных интересов – на английском языке (Field of research: ...).
6. Адрес электронной почты. Убедительная просьба указывать существующий и действующий адрес электронной почты для КАЖДОГО соавтора.
7. Корреспондентский почтовый адрес (с индексом) для контактов с авторами статьи. Данный адрес можно указать один на всех авторов. Можно указать как рабочий (предпочтительно), так и домашний (по желанию) адрес. Обратите внимание на то, что эта информация будет опубликована в открытом доступе.
8. Телефон для связи.

Следует учесть, что данные, приведенные в сведениях об авторах (электронный и обычный адрес, телефоны и факс), должны позволять редакции быстро связаться с авторами статей. Если такая связь оказывается невозможной, то это может привести к задержке в публикации статьи. Следует иметь в виду, что редакция не имеет возможности для ведения длительных междугородних телефонных переговоров. Поэтому настоятельно рекомендуется всю переписку с редакцией вести по электронной почте. Редакция настоятельно рекомендует приводить действующие и часто просматриваемые электронные адреса.

При написании работ просим авторов воспользоваться [рекомендациями по написанию научных статей](#).

Минимальные системные требования:

- процессор: Intel x86, x64, AMD x86, x64 не менее 1 ГГц;
- оперативная память RAM ОЗУ: не менее 512 МБайт;
- свободное место на жестком диске (HDD): не менее 120 МБайт;
- операционная система: Windows XP и выше;
- Adobe Acrobat Reader;
- дисковод CD-ROM;
- мышь.

ООО «Корпорация «Интел Групп»

Системы управления, связи и безопасности

Научный журнал

Адрес редакции:

197372, Санкт-Петербург, пр. Богатырский, д. 32, к. 1 лит. А, пом. 6Н.

Тел.: (812) 945-50-63.

<http://sccs.intelgr.com>

E-mail: sccs@intelgr.com

Свидетельство о регистрации ЭЛ № ФС 77 - 61239 от 03.04.2015 г.

Подписано к использованию 22.03.2017

Объем издания – 9,0 Мб.

Комплектация издания – 1 CD.

Тираж 100 экз.

УДК 681.5

**Воспоминания ветерана инженерной науки:
Пневмоавтоматика. Логическое управление дискретными процессами.
Моделирование сложных дискретных систем**

Юдицкий С. А.

На примере научной биографии автора, охватывающей более полувека, рассмотрены некоторые проблемы управления: пневмоавтоматика как средство автоматизации производственных процессов; логическое управление дискретными процессами на основе графа операций и стандартной позиционной структуры; моделирование сложных систем с применением аппарата индикаторной логики и триадных сетей. Особый акцент при моделировании сделан на двух направлениях, в становлении и развитии которых автор принимал активное участие – моделировании поточных систем обработки мобильных объектов и триадного моделирования дискретных систем. Обзорно представлены методологические основы данных научных направлений, а также показаны прикладные задачи, которые могут быть успешно решены с использованием данного научно-методического аппарата.

Ключевые слова: пневмоавтоматика, логическое управление, сеть Петри, граф операций, позиционная структура, поточная система с мобильными объектами, индикаторная логика, триадная сеть, многоагентная система, триадные дорожные карты.

В 1956 году я закончил Московский станко-инструментальный институт СТАНКИН и в числе группы из 10 выпускников был распределен в Экспериментальный научно-исследовательский институт металлорежущих станков ЭНИМС. В одной из лабораторий ЭНИМСа я писал диплом по исследованию упругих деформаций в плитах – основаниях станков, был очень увлечен этой работой и рассчитывал далее развивать ее. Но по правилам того времени нас всех для приобретения практического опыта на 2 - 3 года отправили на экспериментальный завод «Станкоконструкция», являющийся производственной базой ЭНИМСА. Я оказался в конструкторской группе при отделе главного технолога завода, занимающейся проектированием технологической оснастки – оправок, шаблонов и т.д. Работа вообще не требующая никакой квалификации, да и заявки из цехов на оснастку поступали не часто. Так что конструктора были в основном не загружены, но начальство это несколько не беспокоило. Лишь бы отсиживали положенные рабочие часы. Такая ситуация была типичной для многих предприятий в советское время с конца 50-х.

Смириться я никак не мог, тянуло к исследовательской работе, в науку. На неоднократные просьбы перевести в ЭНИМС получал отказ. Попытался поступить на инженерный поток при Мехмате МГУ. Получил хорошую оценку на собеседовании, но в списке принятых себя не обнаружил. С такой фамилией в те годы на Мехмат (и не только на Мехмат) не брали. В 1958 г. попытался поступить в аспирантуру при ЭНИМСе. На вступительном экзамене по философии на вопрос о культе личности в армии ответил в духе решений 20-го съезда КПСС. Экзаменатор не прерывал, одобрительно кивал. И поставил тройку. Оказывается, надо было сделать упор на «культ маршала Жукова»,

которого незадолго до этого освободили от должности министра обороны. В аспирантуру не приняли.

Наконец, через 2,5 года «работы» на заводе, в апреле 1959 г. меня перевели в ЭНИМС в отдел гидравлики и пневматики. Это начало моей научной биографии. В ЭНИМСе я проработал до 1963 г. Затем поступил в очную аспирантуру при Институте автоматики и телемеханики АН СССР – прежнее название Института проблем управления, где и работаю более полувека. Мой путь в инженерной науке проходил через три проблемные области: пневмоавтоматику, логическое управление дискретными процессами в технических системах, моделирование функционирования сложных систем. В статье далее излагается мое видение проблем этих областей глазами участника работ.

Пневмоавтоматика

В конце 50-х годов зарождалось новое направление в автоматизации дискретных производственных процессов, получившее название «пневмоавтоматика». Функционально дискретные системы пневмоавтоматики соответствовали электрическим релейным схемам, но в качестве рабочей среды в них использовался сжатый воздух. Это обеспечивало защиту от пожаров и взрывобезопасность (в потенциально опасных производствах), повышало надежность, упрощало диагностику неисправностей. Для машин с пневматическим приводом позволяло использовать один вид энергии для выполнения технологических операций и управления. По типу аппаратуры в пневмоавтоматике применялись три вида техники: мембранная, золотниковая, струйная (последнюю также называли пневмоникой). В Советском Союзе работы по пневмоавтоматике, особенно по струйной технике, опережали аналогичные работы за рубежом. Было получено несколько патентов в США и других западных странах. Из ведущих отечественных научных центров пневмоавтоматики на рубеже 50-х и 60-х следует назвать:

- Институт проблем управления (М.А. Айзерман – руководитель работы, группа А.А. Таля – мембранная техника, группа Л.А. Залманзона – струйная техника),
- Институт механизации в подмосковном городе Красноармейск (В.П. Зенченко),
- ЭНИМС (В.И. Щербаков, С.А. Юдицкий - золотниковая техника),
- НИИТЕПЛОПРИБОР (Ю.И. Островский, В.И. Левин – модификация мембранной техники).

В ЭНИМСе я занимался разработкой и апробированием инженерной методики построения систем управления машинами - автоматами (станки, кузнечнопрессовое и литейное оборудование, реакторы периодического действия и т.д.). Суть этой методики заключалась в следующем. Исходным документом являлось графическое описание последовательности работы исполнительных механизмов технологической машины в виде так называемой циклограммы. По циклограмме определялась временная диаграмма действия

сигналов от датчиков, контролирующих состояние исполнительных механизмов (а также другие параметры системы). Далее, на основе логических операций И, ИЛИ, НЕ, ПАМЯТЬ диаграмма датчиков преобразовывалась во временную диаграмму сигналов, управляющих исполнительными механизмами. Последняя корректировалась с учетом нештатных ситуаций и управления машиной в ручном режиме. На всех этапах методики обеспечивалась наглядность (визуализация) и возможность корректировки. Методика совместно с В.И. Щербаковым в 1960 г. была опубликована в журнале «Станки и инструмент» [1], и в 1961 г. перепечатана в английском техническом журнале [2]. В 1962 г. теми же авторами совместно с Л.М. Померанцевым (НИИ авиационной технологии) была опубликована монография [3].

Повышенный интерес к пневмоавтоматике в значительной мере был вызван созданием в 1959-61 гг. в Институте проблем управления (ИПУ) совместно с Московским заводом ТИЗПРИБОР Универсальной системы элементов промышленной пневмоавтоматики УСЭППА. Система представляла собой единый набор унифицированных элементов мембранной техники, на базе которых строились разнообразные управляющие устройства, как дискретные, так и аналоговые. Было организовано промышленное производство приборов на основе УСЭППА на заводе ТИЗПРИБОР. Идеологом и фактическим руководителем разработки и внедрения УСЭППА был Алексей Алексеевич Таль (1920 - 1995), в последующем доктор технических наук, профессор, зав. лабораторией ИПУ, мой научный руководитель в аспирантуре. Создание УСЭППА в 1964 году было отмечено Ленинской премией.

В дальнейшем техника пневмоавтоматики подверглась модернизации: были совмещены в одном элементе мембранная и струйная компоненты (струйно-мембранная техника), элементы размещались на кассетах - стандартных печатных платах с унифицированными разъемами, кассеты помещались в стандартные шкафы. Завод ТИЗПРИБОР освоил выпуск комплекса ЦИКЛ на модернизированной пневматической технике, а на Московском заводе ПНЕВМОАППАРАТ запущено производство созданного при участии ИПУ модернизированного комплекса пневматических агрегатных средств КОМПАС.

Будучи аспирантом (1963 – 65 г.), а затем научным сотрудником ИПУ, я принимал активное участие во всех этих работах, с преимущественной направленностью на разработку эффективных методов графоаналитического описания функционирования технологических объектов управления и построения управляющих устройств на пневматической технике. В 1966 г. защитил кандидатскую диссертацию по этой тематике, в 1968 г. вышла моя монография [4]. В 1968 г. мне поручили возглавить рабочую группу по проектированию и внедрению пневматических систем управления (Т.К. Берендс, Т.К. Ефремова, С. Зарифов, И.Р. Искра, А.А. Тагаевская). Группа работала весьма плодотворно по следующей технологии. Заказчик системы выделял инженера для участия в работе. Совместно с ним составлялось формализованное описание алгоритма функционирования технологической

машины и строилась принципиальная схема управляющего устройства на стандартных кассетах. Далее устройство собиралось на стенде, осуществлялись необходимые коммутации на клеммах кассет (настройка кассет и организация связей между ними), производилось тестирование устройства. Для устройства средней сложности (6 – 8 кассет) весь цикл составлял примерно одну – две недели. За 10 лет (1968-78) через лабораторию прошло больше сотни заказчиков. Кассеты для экспериментальных целей мы получали с завода. Эффективность при создании опытного образца управляющего устройства достигалась в большой степени благодаря принятому способу описания алгоритма (граф операций) и архитектуре управляющего устройства (позиционная структура). Но об этом подробнее в следующем разделе статьи.

Пневмоавтоматика применительно к машинам-автоматам просуществовала более 20 лет и «сошла», не выдержав конкуренции с компьютерами и программируемыми контроллерами. Однако наработанные в пневмоавтоматике методы описания и анализа алгоритмов управления системами инвариантны относительно техники, на которой реализуется управляющее устройство, и сохраняют свою актуальность и поныне.

Логическое управление дискретными процессами

Дискретные процессы, реализуемые в объектах различной природы, состоят из множества целенаправленных действий – операций, выполняемых в некоторой последовательности. Переход от одних операций к другим происходит скачкообразно в дискретные моменты времени и зависит как от продолжительности предыдущих операций и полученных результатов при их выполнении, так и от воздействий внешней среды. Условия перехода между операциями отображаются логическими (булевыми) функциями от переменных, принимающих значения 1 и 0 (истина, ложь). Операции могут выполняться как последовательно, так и параллельно. Задача логического управления дискретными процессами заключается в обеспечении требуемой последовательности операций.

Эффективным и наглядным средством описания и анализа дискретных процессов служит математический аппарат сетей Петри, введенный в 1962 г. немецким математиком К. Петри и развитый в работах ряда ученых (М. Хак [5], Дж. Питерсон [6], В.Е. Котов [7], О.Л. Бандман [8] и др.). Сеть Петри изображается ориентированным графом с двумя типами вершин, где смежными могут быть только вершины разного типа (такие графы называют двудольными). Вершины именуют соответственно позициями (изображаются кружками) и переходами (изображаются планками). В позиции могут помещаться маркеры (фишки), вектор размещения которых по позициям определяет маркирование сети Петри в текущий дискретный момент времени. Для сети задается маркирование в начальный момент, а также финишные маркирования. Если во всех входных позициях перехода есть маркеры, и кроме того, выполняется соотнесенное переходу логическое условие, то переход срабатывает, в результате чего удаляются маркеры из его входных позиций и

вносятся маркеры в выходные позиции. Изменение маркирования сети Петри моделирует динамику дискретного процесса.

Модель дискретного процесса в виде сети Петри, позиции которой соответствуют операциям и помечены управляющими воздействиями на исполнительные органы системы, а переходы соответствуют событиям «Изменение состава выполняемых операций» и помечены логическими условиями, была названа графом операций. Дискретный процесс, моделируемый графом операций, должен удовлетворять ряду условий корректности, в том числе:

- любая операция может быть повторно начата только после своего завершения, т.е. исключается повторное инициирование операции во время ее выполнения;
- из любого маркирования, достижимого из начального, достижимо по меньшей мере одно финишное маркирование, т.е. исключаются зависания и циклы-ловушки, не имеющие выхода.

Анализ дискретных процессов по графу операций подробно рассматривался в монографии автора совместно с В.З. Магергутом [9]. Эта же тематика обсуждалась в моей докторской диссертации, защищенной в ИПУ в 1986 г.

Управляющие устройства на пневматических кассетах собирались непосредственно по графу операций по принципу позиционной структуры: каждой позиции графа сопоставлялась стандартная схемная ячейка, представляющая собой триггер с отдельными входами с предвключенной логикой И – ИЛИ на обоих входах. При построении современных систем логического управления дискретными процессами на электронной технике по графу операций составляется набор причинно-следственных выражений (продукций) вида:

ЕСЛИ <логическое условие> = 1,

ТО включить <список ИО> и выключить <список ИО>,

где формулы логических условий содержат переменные, соотнесенные внешним и внутренним сигналам и операциям, ИО – исполнительные органы системы. Фактически, набор продукций является формальным описанием позиционной структуры. На основе этого набора программируется контроллер или компьютер.

Моделирование сложных дискретных систем

В рамках моделирования сложных систем я занимался проблемами:

- разработки моделей и методов формализованного графоаналитического описания, а также анализа функционирования поточных систем обработки мобильных объектов [10];
- триадного моделирования функционирования дискретных систем [11, 12].

Ниже излагаются основные результаты, полученные в 1992-2012 г.г. при решении этих проблем.

Поточные системы обработки мобильных объектов

Системами такого типа являются промышленные предприятия по выпуску продукции с несколькими переделами (машиностроение, металлургия и др.), ряд социальных систем, где правильнее говорить не об объектах обработки, а о субъектах, свойства (атрибуты) которых могут изменяться при прохождении через систему (например, лечебные учреждения), системы обслуживания заказов населения, и т.д. На вход системы поступают потоки необработанных объектов и потоки ресурсов, необходимых для обработки, на выходе формируются потоки обработанных объектов. Обработка производится с помощью множества операций, причем объекты могут передаваться с операции на операцию. В этом смысле объекты являются мобильными. Ресурсы системы распределяются между операциями. В ходе выполнения операции объект может проходить через несколько стадий, образующих его операционный жизненный цикл. Объектам разного типа могут соответствовать и разные жизненные циклы, являющиеся частными случаями (вариантами) общего операционного цикла. В рассматриваемой модели на операции могут одновременно обрабатываться несколько объектов, находящихся на разных стадиях своего жизненного цикла. Концептуально, операция является конкретизацией понятия «класс» в объектно-ориентированном подходе. Поэтому предлагаемый подход был назван операционно-классовым.

Была разработана методология двухуровневого операционно-классового подхода к моделированию поточных систем. На обоих уровнях модель представляет собой сеть Петри, где позиции соответствуют операциям (классам), а переходы – событиям перемещения мобильных объектов из класса в класс. Для каждого класса дается обобщенный граф операционного жизненного цикла для объектов, обрабатываемых в данном классе. На верхнем, абстрактном, уровне объекты не структурируются, т.е. не указываются их атрибуты. Объекты интерпретируются как маркеры, помещаемые в позиции сети Петри. Различие маршрутов на обобщенном графе жизненного цикла для объектов разного типа игнорируется, моделируется лишь количество объектов на различных стадиях цикла. Хотя модель верхнего уровня и является достаточно грубой, она позволяет частично проверять корректность исходных знаний о функционировании поточной системы и фильтровать ошибки, цена которых на последующих этапах создания системы была бы намного выше.

На нижнем, структурном, уровне моделирования вводятся атрибуты объектов и ресурсов. Для объектов выделяются атрибуты-идентификаторы, значения которых однозначно определяют каждый экземпляр объекта и сохраняются при перемещениях объекта внутри класса и между классами. При структурном моделировании отслеживаются маршруты объектов и динамика их атрибутов, а также расход ресурсов при реализации жизненного цикла каждой операции (пребывании объектов в классе). При переходах некоторые атрибуты могут удаляться и вводиться новые атрибуты («мутация» объектов). В результате структурного моделирования формируется так называемая

конвейерно-временная диаграмма, на которой показан путь каждого мобильного объекта с проекцией на временную ось.

Графоаналитический аппарат абстрактного и структурного моделирования в виде сетей Петри и помечающих их таблиц и логических функций от атрибутов, а также соответствующая методология с иллюстрацией на примерах даны в монографии [10].

Триадное моделирование дискретных систем

В различных предметных областях широко применяются сетевые структуры, представляющие собой множество взаимодействующих автономных функциональных единиц – агентов. Среди факторов, определяющих поведение агента, первостепенными являются: **цели**, зависящие от внутренних ценностей, убеждений и приоритетов агента, а также от складывающейся внешней ситуации; **действия** (операции), направленные на достижение целей; **показатели**, отображающие ключевые параметры агента. Модель агента, выражающая единство и взаимосвязь этих трех факторов, названа триадной, а сетевая структура на базе триадных агентов – многоагентной триадной сетью.

Моделирование триадной сети предусматривает составление ее математического описания, проведение на его основе имитационных экспериментов с выявлением динамических характеристик сети (определение временных и ресурсных характеристик, конфликтных ситуаций, «узких мест» и т.д.) и прогнозированием развития сети на заданном временном горизонте.

Рассмотрим модели и методы формального описания (графового и алгебраического) триадных агентов и сетей. Начнем с определения целей.

Целеполагание заключается в выборе наиболее значимых целей системы и уровней их достижимости исходя из реальных ограничений на ресурсы. При этом последовательно выполняются следующие действия.

Структурирование целей системы. Выделяются главные цели, которые разлагаются на составляющие вплоть до получения элементарных (неразложимых) целей. Целевая структура изображается графом типа дерева, где корневая вершина соответствует главной цели, а вершины-листья соответствуют элементарным целям.

«Взвешивание» элементарных целей – оценивание их числовыми величинами (весами) и ранжирование производится методом анализа иерархий (метод Т. Саати). Дерево целей разбивается на фрагменты, состоящие из корневой вершины с заданным весом (вес главной цели равен 1) и непосредственно подчиненных ей целей, вес которых требуется определить. Для этого попарно сравниваются все подчиненные цели фрагмента, и эксперт оценивает упорядоченные пары. По результатам сравнения и оценки составляется система линейных уравнений, решение которой дает искомые веса подчиненных целей. Далее подчиненная цель, если она не элементарная, принимается за корневую в следующем фрагменте и т.д. Взвешивание начинают с фрагмента, содержащего главную цель.

Минимизация числа элементарных целей с учетом взаимовлияния целей и ограничения на суммарную степень достижимости удаляемых целей (определяется путем экспертной оценки по так называемой когнитивной карте);

Классификация многоцелевых альтернатив. Уровни достижимости элементарных целей из минимизированного множества устанавливаются экспертами и выражаются словесно и в виде числовых оценок. Множество всех возможных наборов уровней достижимости (пространство многоцелевых альтернатив) разбивается на непересекающиеся классы, из которых выбираются приемлемые исходя из состояния ресурсов. Классификация осуществляется методом О.И. Ларичева [13], сочетающим компьютерные процедуры с обращениями к экспертам и позволяющим существенно уменьшить число таких обращений.

Определение в классе доминантной альтернативы (все ее численные компоненты не меньше соответствующих компонент остальных альтернатив класса, но по меньшей мере одна строго больше) и среди доминантных альтернатив всех классов выбирается оптимальная (с максимальным значением интегрального показателя).

Графодинамическая триадная модель агента состоит из связанных между собой двудольных ориентированных графов, позиции которых сопоставлены соответственно целям, действиям и показателям. Позиции графа целей и графа действий описываются булевыми переменными (принимающими значения 0 и 1), графа показателей – арифметическими переменными, принимающими числовые значения в заданном диапазоне. Триадная модель агента определена на дискретной временной шкале с равными промежутками-тактами между заданными моментами наблюдения $\tau = 0, 1, \dots, N$. Предполагается, что любое событие в модели (внешнее воздействие, достижение целей, инициирование и завершение действий, «скачкообразное» изменение показателей) происходит только в моменты τ , которые сопоставляются с переходами на графе действий. В этом смысле дискретная триадная модель является несколько «загрубленной». В реальных сетях события могут происходить и внутри тактов, что требует некоторой коррекции модели.

Временной анализ агента выполняется на основе непрерывно-дискретной модели, в которой действия отображаются на дискретной временной шкале, а показатели на непрерывной. Зависимость показателей от времени с учетом их взаимовлияния описывается многочленными функциями с областью определения на числовой оси. Переходы графа действий срабатывают в граничные моменты между тактами при совпадении трех условий: истечения заданной задержки от момента активирования перехода; наступления внутреннего события на временном интервале, определяемом многочленными функциями и логикой отношений на множестве показателей; наступления внешнего события на этом же интервале. Таким образом, проверяется результативность внешнего события – его влияние (или не влияние) на поведение агента.

Однородность и многоуровневость как расширение триадной структуры агента

В первой версии триадной структуры управление изменением целей и действий являлось «дискретно-событийным» (выполнялось скачкообразно в моменты наступления определенных событий), а управление изменением показателей в соответствии с традициями когнитивного моделирования – «псевдонепрерывным» (управляющие воздействия подаются в каждый момент на горизонте моделирования и зависят от приращения входных показателей переходов графа в предыдущий момент). Такая модель является неоднородной, т.к. для графов целей и действий с одной стороны, и для графов показателей, с другой стороны, применяется разный понятийный и формальный аппарат. В работе вводится однородная триадная структура на основе единого дискретно-событийного аппарата. Агенты реальных сетей могут отличаться большой сложностью – состоять из сотен (и даже тысяч) компонентов, что затрудняет построение модели и ее анализ. Для преодоления барьера сложности традиционно используют иерархическое описание, в частности, на основе стандартов IDEF: описание нижестоящего уровня является детализацией («разверткой») некоторого элемента описания вышестоящего уровня. Недостатком такого подхода является трудность восприятия человеком «картины в целом». Для упрощения восприятия предложено расширение триадной структуры агента, заключающееся в ее многоуровневом линейном представлении с нисходящим расширением и уточнением знаний. Модель строится по «принципу линейки», где графы целей, действий и показателей нижестоящего уровня являются развертками соответствующих графов вышестоящего уровня, т.е. каждый уровень отображает всю систему.

Модель конфигурации сети определяется графом, позиции которого соответствуют агентам, а переходы – взаимодействиям между агентами. Взаимодействие заключается в том, что агент-отправитель, соответствующий входной позиции перехода графа конфигурации, передает некоторый ресурс агентам-получателям (выходным позициям перехода). Если ресурс является материальным или финансовым, то его запас у отправителя при взаимодействии уменьшается на соответствующую величину; если информационным, то база данных отправителя не изменяется.

Динамика развития сети на заданном временном горизонте моделирования

Сеть отображается двухуровневой структурой, где верхний уровень образован графом конфигурации, нижний уровень – триадными моделями агентов. На горизонте моделирования выделяются моменты времени, в которые происходит преобразование графов модели сети, в общем случае на обоих ее уровнях (точки бифуркации). Имитационное моделирование процесса развития сети реализуется в форме диалога введенной модели с Системным архитектором (Лицом, Проводящим Моделирование - ЛПМ). На каждом временном интервале, следующем за моментом преобразования сети, ЛПМ контролирует функционирование модели и фиксирует полученные данные: о

достижении (или не достижении за нормативное время) целей, о тенденциях изменения показателей, о месте и времени нарушений, например, выходе показателей за допустимые пределы, об установлении в сети непредусмотренных циклов и т.д. ЛПМ анализирует эти данные и принимает решение о моменте следующего изменения модели и необходимых преобразованиях графов. Далее процедура повторяется для следующей точки бифуркации и т.д. Результатом имитационного моделирования сети S на горизонте $[0, N]$ является цепочка моделей $S(0), S(1), \dots, S(N)$, где $\tau = 0, 1, \dots, N$ – точки бифуркации на оси времени τ .

Моделирование цикличности развития сетей

Развитие в природе происходит циклически, частным случаем цикла является чередование периодов подъема (расцвета) и спада (увядания). Аналогичное имеет место в экономике и обществе, в том числе в организационных системах, где ведущую роль играет человек (государство и его институты, бизнес-системы, общественные организации). В «организационных сетях» агенты соответствуют подразделениям, которые в период подъема могут «развертываться» – дополнительно создаваться, расширяться, дублироваться с образованием филиалов, а в период спада, наоборот, «свертываться» – с частичной или полной ликвидацией, увольнением персонала и т.д. В условиях цикличности стабильность процессов развития возрастает при увеличении длительности циклов. Следовательно, при имитационном моделировании динамики организационных сетей оправдана постановка задачи поиска варианта развития с наиболее длинными циклами.

Для формирования периодов подъема и спада организационной сети вводится интегральный коэффициент жизнеспособности организации, определяемый по графу конфигурации сети. Коэффициент принимает лингвистические и балльные значения с фиксацией его верхней и нижней границы (лингвистические значения соответствуют словесным формулировкам типа «низкий, средний, высокий» и т.д., балльные значения представлены числами). При моделировании строится ступенчатый график изменения коэффициента жизнеспособности, где ступени соответствуют преобразованию графов конфигурации сети и/или графов агентов в точках бифуркации. Выход графика за верхнюю границу свидетельствует о завершении периода подъема (организация становится слишком сложной и плохо управляемой), а выход за нижнюю границу интерпретируется как кризис (снижение коммутативности и ослабление организации вплоть до прекращения ее существования). Проводятся имитационные эксперименты на моделях циклов с различными параметрами. По результатам экспериментов выбирается цикл максимальной длительности.

Алгебраическое описание структуры и поведения сетей

Модель сети строится в два этапа. Вначале создается ее статическая составляющая, которая для каждого перехода задает входные и выходные позиции. Затем формируется динамическая составляющая модели путем

«нагрузки» переходов продуктами (формулами типа ЕСЛИ→ТО). Статическая составляющая может быть представлена как в графовой, так и в алгебраической форме, с однозначным преобразованием из одной в другую. Графовая форма из-за своей наглядности удобна для сетей малой размерности. Для сложных сетей более эффективно алгебраическое описание в виде строки, составленной из чередующихся символов позиций и переходов и пронумерованных вертикальных стрелок. Длина строки линейно зависит от сложности сети. Такое представление, названное СЛОГ (Структурное Линейное Описание Графов), имеет и ряд других преимуществ: упрощает общение человека с компьютером, в частности ввод данных через клавиатуру, позволяет проводить равносильные преобразования сети, сокращает время компьютерных вычислений.

Для описания динамической составляющей модели сети введен язык индикаторных выражений, являющийся интеграцией продукционных формализмов и формализмов алгебры индикаторных логических формул. Язык обеспечивает:

- однородное описание механизма описания статической и динамической составляющих модели сети (принцип однородности);
- описание продуктов в терминах переменных, соответствующих целям, действиям и показателям сети (принцип триадности);
- описание левой и правой части продукции (условия и действия) на основе индикаторных логических функций;
- описание механизмов взаимодействия агентов в сети путем синхронизации переходов в графах (слогах) агентов и передачи ресурсов от агента к агенту.

Триадные дорожные карты

Дорожные карты представляют собой известный наглядный способ графической интерпретации процессов развития систем различного назначения на долгосрочную перспективу, отражающий различные пути достижения системой экспертно заданного конечного состояния. Разработка дорожных карт является в основном творческим процессом, их согласование и периодическую корректировку рекомендуется проводить в форме экспертных семинаров. В этой связи несомненный эффект дала бы алгоритмизация и последующая компьютеризация процесса построения и анализа дорожной карты с применением интерактивного имитационного моделирования на всех этапах ее жизненного цикла. Суть триадного моделирования заключается в следующем. Ключевыми параметрами процесса развития любой системы являются: цели, к достижению которых стремится развивающаяся система; действия, направленные на достижение целей; показатели, определяющие состояние системы. Параметры отображаются лингвистическо-балльными переменными, характеризующимися словесной и количественной оценкой. Цели, действия и показатели образуют три взаимодействующих уровня модели дорожной карты, где значения переменных, связи между ними, а также связи между уровнями и

связи системы с внешней средой могут изменяться при развитии системы. Каждый уровень моделируется индикаторной сетью – двудольным графом, дополненным продукционными выражениями типа «ЕСЛИ – ТО» на базе индикаторных логических формул (индикаторными выражениями). Совокупность трех упомянутых уровней образует динамическую модель «Триадная дорожная карта (ТДК)». Проводя имитационное моделирование ТДК на заданном временном интервале, получаем описание динамики целей, действий и показателей в дискретном времени.

Анализируемый временной горизонт процесса развития системы (горизонт прогнозирования) состоит из $n \geq 1$ «участков стабильности», на которых изменяются только значения параметров, но остаются неизменными их состав и взаимосвязи. Другими словами, участок характеризуется фиксированной ТДК. Участки стабильности разделены критическими точками, определяемыми как моменты появления «предугрозы» недопустимого нарушения условий работы системы. В критических точках выполняется преобразование ТДК – изменение состава и/или взаимосвязей параметров путем операций над графами и корректировки индикаторных выражений.

Каждому участку стабильности на горизонте моделирования ставится в соответствие ТДК. При этом начальную карту задает ЛПМ. В ходе имитационного моделирования определяются критические точки, в которых ЛПМ трансформирует ТДК предыдущего участка в ТДК последующего участка стабильности. Таким образом, процесс развития в общем случае характеризуется $(n - 1)$ -кратным изменением дорожной карты. Изменение по усмотрению ЛПМ производится на всех трех или лишь на некоторых уровнях карты и носит выборочный характер: выделяется фрагмент графового описания уровня, выделенный фрагмент «вырезается» и замещается другим фрагментом при сохранении преемственности в отношении остальной части графа уровня. Эта процедура подобна медицинской операции и потому названа «графохирургической» операцией.

Триадное моделирование является интерактивным в том смысле, что оно выполняется в форме диалога между компьютером и ЛПМ: компьютер отслеживает функционирование (развитие) системы на участке стабильности и фиксирует появление критической точки («предугрозы»), ЛПМ на основе полученной информации принимает решение и корректирует ТДК.

В заключение статьи поясню смысл использованного в ее названии не очень распространенного словосочетания «инженерная наука». В технических приложениях применяют два стиля изложения материала: строго формальный, базирующийся исключительно на манипуляциях с математическими формулами, и содержательный, с широким использованием различных поясняющих графических конструкций и логическими рассуждениями на естественном языке (русском, английском и т.д.). Инженеру (специалисту с техническим образованием) по мнению автора понятнее второй, инженерный, стиль изложения. В этой связи, термин «инженерная наука» имеет право на

существование. Вместе с тем, следует стремиться к разумному сочетанию обоих стилей.

Литература

1. Щербаков В. И., Юдицкий С. А. Проектирование систем пневмоавтоматики с пневматическим путевым контролем // Станки и инструмент. 1960. № 10.
2. Sherbakov V. I., Yuditskiy S. A. Design of Automatic Systems for Traverse Control // *Compressed Air and Hydraulics*. 1961. №6. №7.
3. Щербаков В. И., Померанцев Л. М., Юдицкий С. А. Пневмоавтоматика в машиностроении. М.: ЦИНТИМАШ, 1962.
4. Юдицкий С. А. Пневматические системы управления приводом машин-автоматов (методы построения). М.: 1968.
5. Hack M. *Decidability Questions for Petri Nets*. New York: Garland Publishing, Inc., 1979
6. Питерсон Дж. Теория сетей Петри и моделирование систем: Пер. с англ. М.: Мир, 1984. 264 с.
7. Котов В. Е. Сети Петри. М.: Наука. Главная редакция физико-математической литературы, 1984. 160 с.
8. Бандман О. Л. Проверка корректности сетевых протоколов с помощью сетей Петри // Автоматика и вычислительная техника. 1986. № 6. С. 82-91.
9. Юдицкий С. А., Магергут В. З. Логическое управление дискретными процессами. Модели, анализ, синтез. М.: Машиностроение, 1987. 176 с.
10. Юдицкий С. А. Сценарный подход к моделированию поведения бизнес-систем. М.: Синтег, 2001. 112 с.
11. Юдицкий С. А. Моделирование динамики многоагентных триадных сетей. М.: Синтег, 2012. 112 с.
12. Юдицкий С. А. Триадно-сетевые дорожные карты развития систем // Управление большими системами. 2013. № 42.
13. Ларичев О. П. Наука и искусство принятия решений. М.: Наука, 1979. 200 с.

References

1. Sherbakov V. I., Yuditskiy S. A. Design of Automatic Systems for Traverse Control. *Machines and Tooling*, 1960, no 10 (in Russia).
2. Sherbakov V. I., Yuditskiy S. A. Design of Automatic Systems for Traverse Control. *Compressed Air and Hydraulics*, 1961, vol 6, no 7.
3. Sherbakov V. I., Pomerantsev L. M., Yuditskiy S. A. *Pnevmoavtomatika v mashinostroenii* [Pneumatic Automation in Mechanical Engineering]. Moscow, Tsentral'nyi nauchno-issledovatel'skii institut mashinostroeniia, 1962 (in Russia).
4. Yuditskiy S. A. *Pnevmaticheskie sistemy upravleniia privodom mashin-avtomatov (metody postroeniia)* [Pneumatic System Management by Actuator of Automatic Machine. Construction Method]. Moscow, 1968 (in Russia).
5. Hack M. *Decidability Questions for Petri Nets*. New York: Garland Publishing, Inc., 1979.

6. Peterson James L. *Petri net theory and the modeling of systems*. The University of Texas at Austin, 1981.
7. Kotov V. E. *Seti Petri* [Petri Nets]. Moscow, Nauka Publ, 1984, pp. 11-58 (in Russian).
8. Bandman O. L. Proverka korrektnosti setevykh protokolov s pomoshch'iu setei Petri [Validation of Network Protocols Using Petri Nets]. *Automatic Control and Computer Sciences*, 1986, vol. 6, pp. 82-91 (in Russian).
9. Iuditskii S. A., Magergut V. Z. *Logicheskoe upravlenie diskretnymi protsessami* [Logical Control of Discrete Processes]. Moscow, Mashinostroenie Publ., 1987 (in Russian).
10. Iuditskii S. A. *Stsenarnyi podkhod k modelirovaniu povedeniia biznes-sistem* [Scenario Approach to Modelling for Business Systems]. Moscow, Sinteg Publ., 2001 (in Russian).
11. Iuditskii S. A. *Modelirovanie dinamiki mnogoagentnykh triadnykh setei* [Modeling the Dynamics of Multi-Agent Triadic Nets]. Moscow, Sinteg Publ., 2012 (in Russian).
12. Iuditskii S. A. The triadic-networked roadmaps for systems development. *Large-scale Systems Control*, 2013, vol 42 (in Russian).
13. Larichev O. P. *Nauka i iskusstvo priniatiia reshenii* [The Science and Art of Decision Making]. Moscow, Nauka Publ., 1979, 200 p. (in Russian).

Статья поступила 22 июня 2015 г.

Информация об авторе

Юдицкий Семен Абрамович - доктор технических наук, профессор, главный научный сотрудник. Институт проблем управления им. В.А. Трапезникова. Область научных интересов: моделирование организационно-технических систем. Тел. +7 495 339 59 10. E-mail: yuseab32@yandex.ru

Адрес: Россия, 117997, Москва ул. Профсоюзная, д. 65.

Memories of Veteran Engineering: Pneumatics, Logical Control of Discrete Processes, Modeling Complex Discrete Systems

Iuditskii S. A.

Some issues of control are described in article. Pneumatics as a means of automation of production processes; logical control of discrete processes at the basis of the graph operations and standard positional patterns; modeling of complex systems using the formal apparatus of the indicator logic and triadic networks is considered on the example of a scientific biography of the author, covering more than half a century. Modeling of stream processing systems of mobile objects and triadic modeling of discrete systems are discussed in detail. Applied problem that can be successfully solved with the use of this scientific-methodical machines is shown by the author in the paper.

Key words: *Pneumatics, logic management, Petri nets, graph operations, positional structure, the in-line system with mobile objects, display logic, triad network, multi-agent system, process road map.*

Information about Author

Iuditskii Semen Abramovich - Dr. habil. of Engineering Sciences, Full Professor, Senior Research Officer. Institute of Control Sciences RAS. Field of research: modeling of organizational and technical systems. Tel.:+7 495 339 59 10. E-mail: yuseab32@yandex.ru

Address: Russia, 117997, Moscow, Profsoyuznaya str., 65.

УДК 621.396

Метод кодового уплотнения скрытого канала при передаче видеоданных

Абазина Е. С.

Актуальность работы: увеличение количества информационных направлений связи одновременно функционирующих в скрытом (стеганографическом) канале в структуре одного мультимедийного контейнера актуализирует вопросы обеспечения применимости методов цифровой стеганографии для более широкого класса задач. Известные способы стеганографического обмена не позволяют организовать более одного информационного направления связи в скрытом канале передачи данных в мультимедийном потоке. **Целью работы** является повышение числа информационных направлений связи в скрытом канале при передаче видеоданных при ограничениях на достоверность приема скрываемых данных, передаваемых в каждом информационном направлении, и скрытность встраивания. **Используемые методы:** предлагается применить кодовое уплотнение данных как технологию, позволяющую достичь компромисса в противоречии между скрытностью встраивания, пропускной способностью скрытого канала и достоверностью приема скрываемых данных. **Постановка задачи:** разработать метод кодового уплотнения скрытых каналов в структуре видеоданных. **Новизна:** элементами новизны представленного решения являются: проведение дополнительных этапов стеганографической обработки контейнера и встраиваемых данных каждого из информационных направлений связи, состоящих как в реализации кодового уплотнения до сжатия видеоданных с применением двумерных шумоподобных сигнальных конструкций, так и проведением двойного ортогонального преобразования видеоданных с одновременным встраиванием согласованных с ним двумерных модулированных сигнальных конструкций. Также к элементу новизны стоит отнести способ разделения информационных направлений связи в скрытом канале, определение ключевых данных и порядок размещения скрываемых данных в кадре изображения-контейнера. **Результат:** использование разработанного метода кодового уплотнения скрытых каналов в структуре видеоданных позволяет увеличить число информационных направлений связи в скрытом канале минимум в три раза (при скрытой пропускной способности каждого информационного направления связи скрытого канала не менее 1,2 кбит/с и вероятности ошибочного приема скрываемых данных не хуже 10^{-3}) и зависит от уровня качества видеоданных. Максимум скрытой пропускной способности уплотненного скрытого канала не превышает 20% от пропускной способности канала передачи видеоданных. **Практическая значимость:** заключается в доведении разработанного научно-методического аппарата до реализуемых алгоритмов, которые позволяют использовать результаты исследований при разработке кодера видеоданных.

Ключевые слова: видеоданные, стандарты сжатия JPEG, MPEG-2, стеганография, двумерные шумоподобные сигнальные конструкции, кодовое уплотнение (разделение) данных.

Введение

«Кто владеет информацией – тот владеет миром» – эти слова, всегда отражавшие ценность обладания сведениями, стали буквально девизом последнего столетия, и как нельзя лучше говорят необходимости защиты информации от несанкционированных пользователей сегодня. Цифровая стеганография, получившая в последние десятилетия активное развитие, позволяет решать задачу сокрытия сведений в объектах, имеющих аналоговую природу (изображения, видео, звуки) и представленных в цифровом виде. Анализ основополагающих работ [1, 2] в этой области показал, что в большинстве исследований рассматривается лишь один скрытый канал, без учета возможности его разделения между абонентами, или предоставления к нему множественного доступа. Идея разработки предложений по уплотнению

(разделению) скрытого канала является логичным направлением развития стеганографической науки.

В настоящее время в области стеганографии в Российской Федерации не предусмотрено государственных стандартов и норм, определяющих терминологию. В опубликованных работах по этой тематике одни и те же термины имеют различные значения. И наоборот, одним и тем же понятиям поставлены в соответствие разные определения. В связи с этим, уточним используемый в работе терминологический базис.

Скрытой передачей информации называют процессы, реализующие методы передачи информации, при которых возможна передача дополнительной информации в структуре данных, представленных в цифровом виде и используемых в качестве контейнера, а также за счет их избыточности.

Под *контейнером* (покрывающим объектом) понимают такие цифровые данные, использование избыточности которых позволяет передавать дополнительную информацию, не обнаруживая факта передачи. Контейнер, не содержащий дополнительной информации, является *пустым*, в противном случае – *заполненным*.

В работе в качестве контейнера выбраны видеоданные наиболее популярных форматов (JPEG, MPEG-2). Выбор неподвижных и подвижных изображений обоснован их большой психовизуальной избыточностью.

Совокупность методик и средств встраивания и извлечения дополнительной информации без обнаружения нарушения целостности контейнера потребителем позволяет говорить о формировании *скрытого канала* (СК) передачи информации.

Стеганографической системой (*стегосистемой*) в работе называется совокупность средств и методов передачи и приема пустого контейнера, функционирующих взаимосвязано со средствами и методами, используемыми для создания скрытого канала передачи информации.

Под *информационным направлением связи* (ИНС) скрытого канала понимается логическое соединение пары абонентов – участников скрытого информационного обмена.

В случае организации в одном скрытом канале более одного ИНС, скрытый канал называется *уплотненным*.

Основными характеристиками СК, состоящими в противоречии друг с другом, являются скрытая пропускная способность СК и скрытность (стеганографическая стойкость).

Скрытая пропускная способность имеет смысл максимального количества информации, которое возможно передать с заданной достоверностью при одном использовании контейнера. Ограничением скрытой пропускной способности являются искажения, вносимые в контейнер при встраивании дополнительной информации, которые в работах [1, 2] называются *искажениями кодирования*. Требования по достоверности скрыто передаваемой информации также влияют на верхнюю границу скрытой пропускной способности, снижая ее. Учитывая введенное определение ИНС СК, а также по

аналогии с системой связи, скрытая пропускная способность также может быть оценена числом ИНС в одном СК.

Скрытность (стеганографическая стойкость) определяется возможными действиями (атаками) нарушителя в отношении стегосистемы. В настоящей работе рассмотрена ситуация, когда нарушитель не имеет априорных сведений о наличии в видеопотоке скрытого канала. Таким образом, здесь под *скрытностью* понимается устойчивость скрытого канала к факту обнаружения. Атаки, предпринимаемые нарушителем будут иметь пассивный характер, и могут выражаться в проведении следующих мероприятий:

- визуальный контроль с целью субъективной оценки качества видеоданных;
- объективный контроль видеоданных по одному (или нескольким) выбранному параметру оценки качества изображений;
- гистограммная атака.

Вопросы организации множественного доступа к скрытому каналу являются логичным продолжением развития системы взглядов цифровой стеганографии. Разработка же методов уплотнения скрытого канала позволит расширить область применения стеганографической науки при обеспечении безопасности информационного обмена.

Анализ общетехнических требований, предъявляемых к каналам связи специального назначения, позволил установить, что минимальная пропускная способность одного ИНС СК должна составлять не менее 1,2 кбит/с при вероятности ошибочного приема скрываемых данных 10^{-3} . Минимальное число ИНС, необходимых для обеспечения скрытого обмена в пределах типового учреждения, составляет 5 низкоскоростных каналов, два из которых являются каналами низкоскоростной передачи данных (со скоростью до 100 бит/с), а три – речевые каналы с качеством разборчивости речи не хуже «удовлетворительно». Требование к скрытой пропускной способности уплотненного СК соответствует 4 кбит/с [3].

Основным недостатком известных подходов [1, 2] организации скрытых каналов в видеоданных является их низкая пропускная способность и невозможность организации более одного скрытого канала в структуре одного видеопотока. Одним из компромиссных решений в этом случае, удовлетворяющим требованиям по пропускной способности и помехозащищенности, может выступать кодовое уплотнение.

Обзор отечественной и иностранной литературы, посвященной скрытой передаче информации, показал, что вопросам внедрения информации в видеоданные посвящено большое количество работ. В данном направлении выполнены работы Оковым И.Н., Грибуниным В.Г., Конаховичем Г.Ф., Пузыренко А.Ю., Кохом Е., Жао Дж., Марвелом Л. и другими. Вопросами использования шумоподобных сигналов и оптимальных преобразований при встраивании посвящены работы Цветкова К.Ю., Коревых А.Е., Коровина В.М. Вместе с тем, организацией кодового уплотнения для устранения основного недостатка известных подходов по построению скрытых каналов передачи информации уделено недостаточно внимания. Поэтому вопросы организации

кодowego уплотнения скрытых каналов при передаче видеоданных представляются актуальными. Анализ основных подходов к организации скрытых каналов видеоданных представлен в таблице 1.

Таблица 1 – Сравнительный анализ известных методов скрытой передачи информации в видеоданных

Классификация методов организации скрытых каналов в видеоданных		Правило встраивания ρ	Пропускная способность скрытого канала $C_{стег}$	Скрытность U	Достоверность скрываемых данных $P_{ош}$	Число скрытых каналов
1. Направление цифровой стеганографии – встраивание цифровых водяных знаков (ЦВЗ) с целью подтверждения данных						
2. Направление цифровой стеганографии – организация скрытого канала с целью сокрытия факта передачи						
В пространственной области	Наименее значащего бита					
	К.Ю.Цветков, В.М.Коровин, К.Матсуи, К.Танака, С.Осборн, Дж.Фридрих	$\rho^1 = I + S$	$C^1_{стег} = \max$	$U^1 = \min$	$P_{ош} = 10^{-3}$, без сжатия	1
	Псевдослучайного интервала (Д.Рамкуман, Дж.Симонс, В.Волошиновский)	$\rho^2 = I + S I_h = 1$	$C^2_{стег} < C^1_{стег}$	$U^2 > U^1$	$P_{ош} = 10^{-3}$, без сжатия	1
	Псевдослучайной перестановки (В.И. Коржик, С.Моллер, А.Фицманн, И.Стиран)	$\rho^3 = I + S h = \varphi_i$, φ_i – ПСП	$C^3_{стег} < C^2_{стег}$	$U^3 > U^2$	$P_{ош} = 10^{-3}$, без сжатия	1
	Блочного скрывания (В.О.Хорошко, О.Д.Азаров, К.Ю. Цветков, В.М.Коровин)	$\rho^4 = \left(\frac{I}{D}\right) + S$, D – число блоков	$C^4_{стег} \approx C^3_{стег}$	$U^4 > U^3$	$P_{ош} = 10^{-3}$, без сжатия	1
В частотной области	Наименее значащего бита					
	В.Г.Грибунин, К.Ю.Цветков, В.М.Коровин, Е.Кох	$\rho^5 = I^{ДКП} + S$	$C^5_{стег} = \max$	$U^5 > U^1$	$P_{ош} = 10^{-3}$, без сжатия	1
	Относительной замены	$\rho^6 = \begin{cases} S_0, \left(\frac{I^{ДКП}}{D}\right)_1 - \left(\frac{I^{ДКП}}{D}\right)_2 > P \\ S_1, \left(\frac{I^{ДКП}}{D}\right)_1 - \left(\frac{I^{ДКП}}{D}\right)_2 < P \end{cases}$, P – порог	$C^6_{стег} < C^4_{стег}$	$U^6 \approx U^4$	$P_{ош} = 10^{-3}$, в процессе сжатия	1
	Бенгама-Меммона (Д.Бенгам, Н.Меммон, Б-Л Эо, М. Юнг)	$\rho^7 = \begin{cases} S_0, \left\{ \left(\frac{I^{ДКП}}{D}\right)_3 < \left(\frac{I^{ДКП}}{D}\right)_1 \right. \\ \left. \left(\frac{I^{ДКП}}{D}\right)_3 < \left(\frac{I^{ДКП}}{D}\right)_2 \right\} \\ S_1, \left\{ \left(\frac{I^{ДКП}}{D}\right)_3 > \left(\frac{I^{ДКП}}{D}\right)_1 \right. \\ \left. \left(\frac{I^{ДКП}}{D}\right)_3 > \left(\frac{I^{ДКП}}{D}\right)_2 \right\} \end{cases}$	$C^7_{стег} < C^6_{стег}$	$U^7 > U^6$	$P_{ош} = 10^{-3}$, в процессе сжатия	1
	Фридрих	$\rho^8 = (I)^{ДКП} + S (I')^{ДКП} < (I)^{ДКП} + 10^2 \alpha$, I' – модифицированные видеоданные, α – пороговая функция	$C^8_{стег} < C^7_{стег}$	$U^8 \approx U^7$	$P_{ош} = 10^{-3}$, в процессе сжатия	1
	Расширения спектра	$\rho^{10} = (I)^{ДКП} + S \cdot \varphi_i$, φ_i – ПСП	$C^8_{стег} < C^{10}_{стег} < C^1_{стег}$	$U^{10} \approx U^9$	$P_{ош} = 10^{-3}$, в процессе сжатия	1
	К.Ю.Цветков, А.Е.Коревых, В.М.Коровин, Дж.-Р. Смит, В.О.Комиски					
Статистический (И. Патис, В.О.Хорошко, В.Г.Грибунин, М.Е. Шелест)		$\rho^9 = \left[(I)_1^{ДКП}\right]^{\frac{E}{2}} \cup \left[(I)_2^{ДКП}\right]^{\frac{E}{2}}$, E – энергия изображения	$C^9_{стег} < C^8_{стег}$	$U^9 > U^8$	$P_{ош} = 10^{-3}$, в процессе сжатия	1

Объектом исследования является скрытый канал передачи информации в видеоданных, предметом исследования – кодирование уплотнение скрытого канала при передаче видеоданных.

Противоречие в науке заключается в противоречии между скрытностью встраивания, пропускной способностью скрытого канала и достоверностью приема данных, передаваемых в скрытом канале, противоречие в практике – в

отсутствии множественного доступа к скрытому каналу в условиях организации скрытого обмена между несколькими абонентами.

Таким образом, *научная задача* исследования состоит в разработке научно-методического аппарата кодового уплотнения скрытого канала при передаче при ограничениях на достоверность приема и скрытность встраивания.

Целью работы является повышение числа ИНС СК при передаче видеоданных при ограничениях на достоверность приема и скрытность встраивания.

Для достижения поставленной в работе цели необходимо решить следующие *частные задачи*:

- разработать модель кодового уплотнения скрытого канала при передаче видеоданных;
- предложить алгоритмы кодового уплотнения, встраивания и извлечения данных скрытого канала из видеоданных;
- выработать предложения по совершенствованию кодера видеоданных.

Постановка и формализация научной задачи исследования

Научная задача исследования заключается в разработке научно-методического аппарата кодового уплотнения скрытого канала при передаче видеоданных, позволяющего повысить число ИНС СК при ограничениях на достоверность приема и скрытность встраивания [3]:

$$K_{\text{скр}}(I, \rho, S, \Phi, m, \theta) \left\| \begin{array}{l} \max, \\ I' \in U, S \in V \end{array} \right.$$

где $K_{\text{скр}}$ – число ИНС СК в видеопотоке, зависящее от исходных видеоданных I , правила встраивания скрытого канала ρ , скрываемых данных S , используемых для сокрытия сигнальных конструкций Φ , их значности m и коэффициента встраивания θ ;

$I' \in U, U = \{R(I'), \text{hist}(I'), q(I')\}$ – множество ограничений на скрытность встраивания, где I' – модифицированные видеоданные (заполненный контейнер), $R(I') \geq 25 \text{ дБ}$ – пиковое отношение сигнал-шум модифицированных видеоданных, $\text{hist}_{\text{max}}(I') \neq 2\theta$ – изменение гистограммы модифицированных видеоданных, отсутствие раздвоения пика, $q(I')$ – усредненная субъективная оценка визуального качества модифицированных видеоданных;

$S_k \in V, V = \{C_{\text{скр}}(S_k), p_{\text{ош}}(S'_k), k\}$ – множество ограничений на достоверность приема скрываемых данных, где S'_k – данные, передаваемые по каждому из ИНС СК, на приемной стороне, $C_{\text{скр}}(S_k) \geq 1,2 \text{ кбит/с}$ – минимальная пропускная способность одного ИНС СК; $p_{\text{ош}}(S'_k) \leq 10^{-3}$ – вероятность ошибочного приема на бит данных, передаваемых по каждому из ИНС СК, $k \geq 5$ – число ИНС в одном видеопотоке.

Модель кодового уплотнения скрытого канала при передаче видеоданных

В работе проведено исследование спектральных характеристик шумоподобных сигнальных конструкций в мультипликативных базисах [4, 5], разработана структура метода кодового уплотнения скрытого канала при передаче видеоданных [6], а также разработана модель кодового уплотнения скрытого канала [7-10] и проведено оценивание скрытности встраивания уплотненного скрытого канала в видеоданные [11].

Для разработки метода кодового уплотнения скрытых каналов в качестве прототипа был выбран метод организации скрытых каналов с применением шумоподобных сигналов [9]. Существенным недостатком данного метода, является принципиальная возможность организации не более одного ИНС СК в видеопотоке. Минимальные же требования, определенные в работе, оцениваются пятью каналами с суммарной пропускной способностью 4 кбит/с, при пропускной способности одного ИНС СК не менее 1,2 кбит/с и при достоверности приема данных не хуже 10^{-3} . Кроме того, анализ выбранного метода показал, что его применение в отношении видеоданных приводит к искажению гистограммы, выражающемуся в раздвоении главного пика. Причем, расстояние между двумя пиками модифицированного изображения тем больше, чем больше коэффициент встраивания θ . Предлагаемый новый метод кодового уплотнения скрытого канала при передаче видеоданных основывается на новой оригинальной модели кодового уплотнения скрытого канала, которая учитывает как противоречивые требования организации скрытых каналов, так и особенности технологии передачи видео. Данная модель, являющаяся выражением системы взглядов автора на организацию кодового уплотнения скрытого канала, позволяет организовать встраивание в видеоданные более одного ИНС СК при ограничениях на скрытность встраивания (рис. 1). Модель включает в себя аналитическое представление операций следующих этапов:

- выбор комбинации, состоящей из двумерной шумоподобной сигнальной конструкции и ортогонального преобразования;
- формирование уплотненного скрытого канала;
- проведение двойных спектральных преобразований видеоданных;
- встраивание уплотненного скрытого канала в видеоданные.

Выбор комбинации двумерной шумоподобной сигнальной конструкции $(\Phi_{if}(g) = [\varphi_{if}(g)]$ с периодом N ($N = n^s$, $n \geq 2$, $s \geq 1$) и ортогонального преобразования осуществляется одноименной группой блоков модели кодового уплотнения скрытого канала (рис. 1).

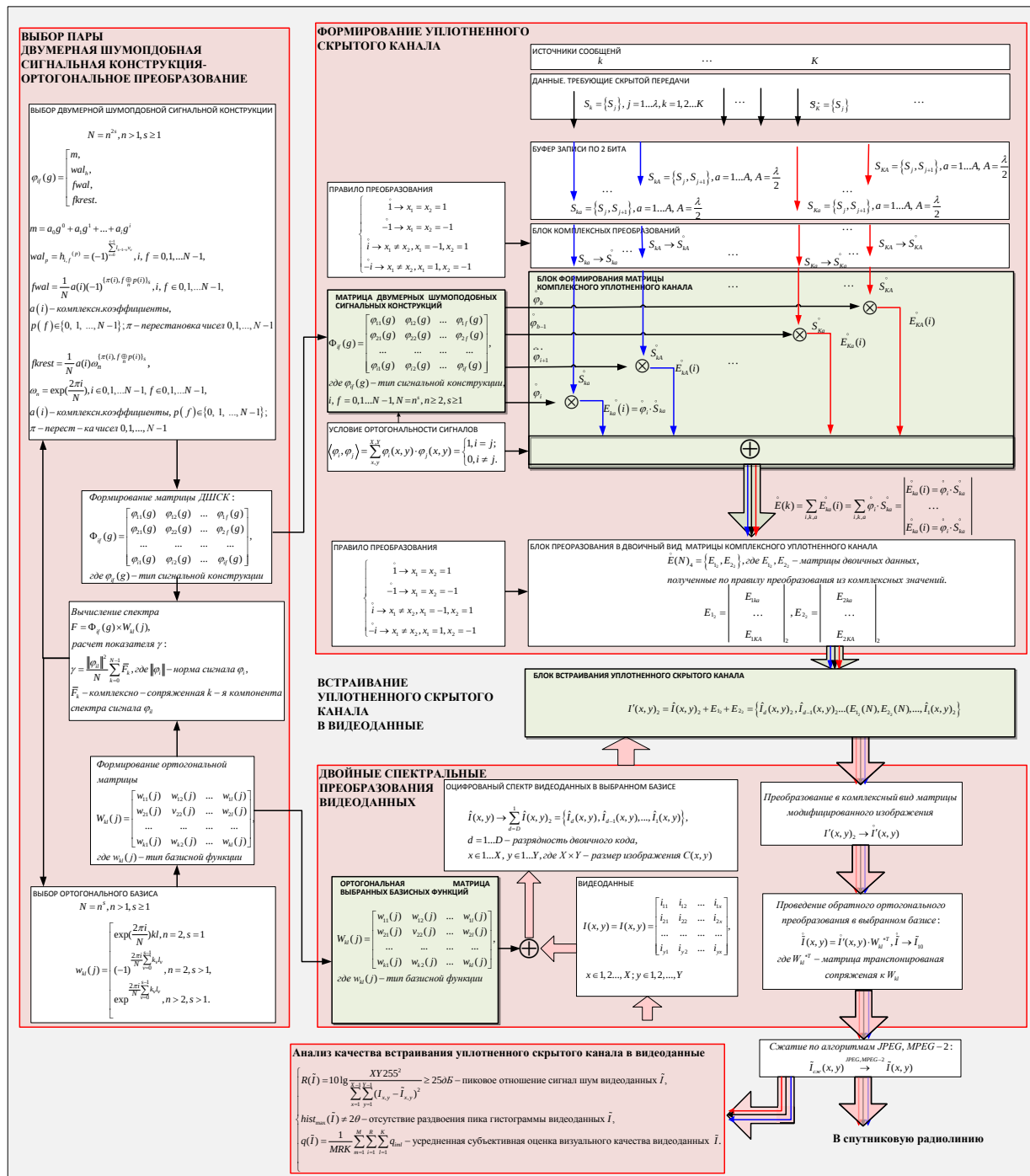


Рис. 1. Модель кодового уплотнения скрытых каналов управления войсками в видеоданных

Исходными сигнальными конструкциями ($\varphi_{if}(g)$), рассматриваемыми в работе, являются:

$$\varphi_{if}(g) = \begin{cases} m, \\ wal_h, \\ fwal, \\ fkrest. \end{cases}$$

где $m = a_0 g^0 + a_1 g^1 + \dots + a_i g^i$ – M -последовательность, заданная порождающим полиномом; $wal_h = h_{i,f}^{(h)} = (-1)^{\sum_{v=0}^{s-1} i_v f_v}$, $i, f = 0, 1, \dots, N-1$ – сигнальные конструкции Уолша, упорядоченные по Адамару (У-А), где i, f – порядковые номера базисной функции и аргумент этой функции соответственно, $N = n^s$, $n = 2$, $s > 1$ – период функций; $fwal = \frac{1}{N} a(i) (-1)^{\{\pi(i), f \oplus_n p(i)\}_s}$, $i, f \in 0, 1, \dots, N-1$ – сигнальные конструкции Франка-Уолша (Ф-У), где $a(i)$ – комплексные коэффициенты, $p(f) \in \{0, 1, \dots, N-1\}$; π – перестановка чисел $0, 1, \dots, N-1$; $fkrest = \frac{1}{N} a(i) \omega_n^{\{\pi(i), f \oplus_n p(i)\}_s}$ – сигнальные конструкции Франка-Крестенсона (Ф-К), где $\omega_n = \exp\left(\frac{2\pi i}{N}\right)$, $i \in 0, 1, \dots, N-1$, $f \in 0, 1, \dots, N-1$, $a(i)$ – комплексные коэффициенты, $p(f) \in \{0, 1, \dots, N-1\}$; π – перестановка чисел $0, 1, \dots, N-1$, $N = n^s$, $n > 2$, $s > 1$.

Матрица двумерных шумоподобных сигнальных конструкций (ДШСК) формируется путем сдвига выбранной сигнальной конструкции. Так, для M -последовательности и сигнальных конструкций У-А естественным сдвигом является циклический сдвиг, для сигнальных конструкций Ф-У – диадный, а для Ф-К – n -сдвиг. В результате общий вид матрицы ДШСК имеет вид:

$$\Phi_{if}(g) = \begin{bmatrix} \varphi_{11}(g) & \varphi_{12}(g) & \dots & \varphi_{1f}(g) \\ \varphi_{21}(g) & \varphi_{22}(g) & \dots & \varphi_{2f}(g) \\ \dots & \dots & \dots & \dots \\ \varphi_{i1}(g) & \varphi_{i2}(g) & \dots & \varphi_{if}(g) \end{bmatrix},$$

где $\varphi_{if}(g)$ – тип выбранной сигнальной конструкции.

Для проведения предварительного ортогонального преобразования выбирается базис:

$$w_{kl}(j) = \begin{cases} \exp\left(\frac{2\pi i}{N}\right) kl, & n = 2, s = 1 \\ (-1)^{\frac{2\pi i}{N} \sum_{v=0}^{s-1} k_v l_v}, & n = 2, s > 1 \\ \exp\left(\frac{2\pi i}{N} \sum_{v=0}^{s-1} k_v l_v\right), & n > 2, s > 1 \end{cases},$$

где базис функций В-К является обобщением для случаев ДЭФ и функций Уолша, получаемых при значениях $n = 2, s = 1$ и $n = 2, s > 1$ соответственно. Для проведения дальнейших операций кодового уплотнения скрытых каналов спектр каждого ДШСК в каждом из базисов оценивается путем вычисления коэффициента дельта-корреляции γ : $\gamma = \frac{\|\varphi_i\|^2}{N} \sum_{k=0}^{N-1} \bar{F}_k$, где $F = \Phi_{if}(g) \times W_{kl}(j)$ – спектр ДШСК в выбранном базисе, $\|\varphi_i\|$ – норма сигнала φ_i , $\bar{F}_k$ – комплексно-сопряженная k -я компонента спектра сигнала φ_i .

Коэффициент γ характеризует близость структуры спектра сигнала к шумоподобному и принимает наименьшее значение, равное единице, для дельта-коррелированных сигналов с равномерным спектром.

Принцип формирования уплотненного скрытого канала заключается в использовании ортогональной матрицы ДШСК, обеспечивающей кодовое уплотнение сигналов от абонентов. В зависимости от количества источников скрывааемых сообщений входные данные кодируются ортогональными сигналами матрицы ДШСК путем модуляции информационными элементами сигналов абонентов строк матрицы ДШСК.

Все используемые ДШСК имеют значность $m=2$, при выборе же ДШСК Ф-К $m>2$, в частном случае, рассматриваемом в диссертации, $m=4$, что соответствует комплексному представлению $(\dot{\varphi}_i = \{1, -1, i, -i\})$. Входные информационные сигналы K абонентов, обозначим их $S_k = \{S_j\}, j=1...\lambda, k=1...K$, представляют собой вектора из $j=1...\lambda$ бит информации.

Каждая пара бит $(S_j, S_{j+1})_k$ сообщения k -ого абонента, кодируется укрупнением и представляется соответствующим комплексным значением $S_{ka} \rightarrow \dot{S}_{ka}, S_{ka} = \{S_j, S_{j+1}\}, a=1...A, A=\frac{G}{2}$, каждое из которых представляется некоторой базисной функцией φ_i с периодом N .

Комплекснозначное модулированное сообщение от k -ого абонента, при использовании ДШСК Ф-К, имеет формальное представление:

$$\dot{E}(k) = \sum_{i,k,a} \dot{E}_{ka}(i) = \sum_{i,k,a} \dot{\varphi}_i \cdot \dot{S}_{ka} = \begin{bmatrix} \dot{E}_{ka}(i) = \dot{\varphi}_i \cdot \dot{S}_{ka} \\ \dots \\ \dot{E}_{ka}(i) = \dot{\varphi}_i \cdot \dot{S}_{ka} \end{bmatrix}.$$

Для обеспечения возможности встраивания сформированных уплотненных ИНС СК в изображение-контейнер, представленный в двоичном коде, уплотненные ИНС СК преобразуются в двоичный вид: $\dot{E}(N)_4 = \{E_{1_2}, E_{2_2}\}$, где E_{1_2}, E_{2_2} – матрицы сформированных уплотненных ИНС СК в двоичном коде. Перед встраиванием и проведением процедур сжатия по форматам JPEG, MPEG-2 исходные видеоданные вида:

$$I_B(x, y) = \begin{bmatrix} i_{11} & i_{12} & \dots & i_{1x} \\ i_{21} & i_{22} & \dots & i_{2x} \\ \dots & \dots & \dots & \dots \\ i_{y1} & i_{y2} & \dots & i_{yx} \end{bmatrix}, x \in 1, 2, \dots, X, y \in 1, 2, \dots, Y,$$

переводятся из пространственной области в частотную путем проведения прямого ортогонального преобразования в выбранном базисе. Для этого матрицу видеоданных необходимо умножить на ортогональную матрицу выбранного базиса вида:

$$W_{kl}(j) = \begin{bmatrix} \omega_{11}(j) & \omega_{12}(j) & \dots & \omega_{k1}(j) \\ \omega_{21}(j) & \omega_{22}(j) & \dots & \omega_{k2}(j) \\ \dots & \dots & \dots & \dots \\ \omega_{l1}(j) & \omega_{l2}(j) & \dots & \omega_{kl}(j) \end{bmatrix}, k, l = 1, 2, \dots, M.$$

Спектр в базисе В-К в матричном виде может быть представлен $\bar{I} = I \cdot W$. Так как прямое ортогональное преобразование В-К над видеоданными двумерно, коэффициенты преобразования могут быть представлены матрицей, каждый из которых имеет вид суммы битовых плоскостей в двоичном коде:

$\bar{I}(x, y) \rightarrow \sum_{d=D}^1 \bar{I}(x, y)_2 = \{\bar{I}_d(x, y), \bar{I}_{d-1}(x, y), \dots, \bar{I}_1(x, y)\}$, где $d=1 \dots D$ – разрядность двоичного кода видеоданных $I(x, y)$.

Встраивание матрицы уплотненных ИНС СК осуществляется заменой одного или нескольких битов коэффициентов оцифрованного спектра видеоданных в выбранном базисе значениями сформированных матриц E_{1_2}, E_{2_2} :

$$\bar{I}(x, y)_2 = \bar{I}(x, y)_2 + E_{1_2} + E_{2_2} = \{\bar{I}_d(x, y)_2, \bar{I}_{d-1}(x, y)_2, \dots, E_{1_2}(N), E_{2_2}(N), \dots, \bar{I}_1(x, y)_2\}.$$

В дальнейшем, заполненный видеоконтейнер переводится в комплексный вид $I'(x, y)_2 \rightarrow \overset{\circ}{I}'(x, y)$ и проводится обратное ортогональное преобразование в базисе В-К путем умножения на транспонированную комплексно-сопряженную матрицу в базисе В-К W_{kl}^{*T} : $\overset{\circ}{I}'(x, y) = \overset{\circ}{I}'(x, y) \cdot W_{kl}^{*T}, \overset{\circ}{I}' \rightarrow \tilde{I}_{10}$.

В результате имеем видеоданные со встроенным уплотненным скрытым каналом, которые затем подвергаются алгоритмам сжатия в соответствии с форматами JPEG, MPEG-2:

$$\tilde{I}_{сж}(x, y) \xrightarrow{JPEG, MPEG-2} \tilde{I}(x, y).$$

На приемной стороне производятся обратные операции.

Таким образом, в результате проведенных исследований и расчетов разработана аналитическая модель кодового уплотнения скрытого канала при передаче видеоданных, отличающаяся от известных проведением дополнительных этапов, состоящих как в реализации кодового уплотнения ИНС СК до сжатия видеоданных на основе двумерных шумоподобных сигнальных конструкций, так и в проведении двойного ортогонального преобразования видеоданных с одновременным встраиванием согласованной двумерной модулированной сигнальной конструкции.

Проведено исследование спектральных характеристик ДШСК при проведении ортогональных преобразований в различных базисах. Проведено оценивание скрытности встраивания видеоданных по следующим параметрам, определенным при постановке и формализации задачи:

- изменение гистограммы видеоданных после встраивания, отсутствие раздвоения пика $hist_{\max}(I') \neq 2\theta$ (таблица 2);
- усредненная субъективная оценка визуального качества видеоданных $q(I')$, с качеством восприятия не хуже хорошего – оценивание

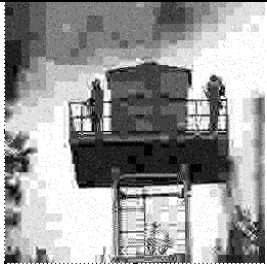
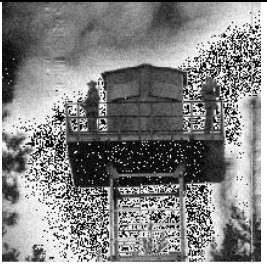
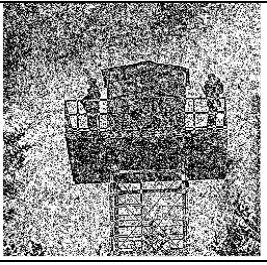
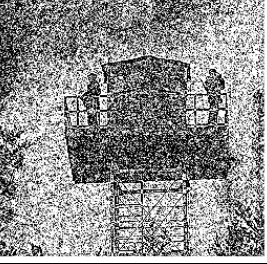
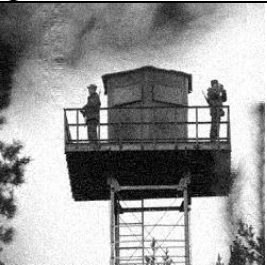
проводилось группой экспертов в соответствии с ГОСТ 26320-84 (таблица 3);

- пиковое отношение сигнал-шум (ПОСШ) видеоданных после встраивания $R(I') \geq 25$ дБ, результаты расчета ПОСШ оценивались в соответствии с ГОСТ Р 52722-2007 (рис. 2).

Таблица 2 – Деградация гистограммы изображения при встраивании

Пара бит 1 и 2	Пара бит 4 и 5	Пара бит 10 и 11	Тройка бит 1,2 и 3
Гистограммы изображения при встраивании после сжатия JPEG			
Гистограммы изображения при встраивании в процессе сжатия JPEG			
Гистограммы изображения при встраивании до сжатия JPEG, с проведением предварительного ДКП			
Гистограммы изображения при встраивании до сжатия JPEG, с проведением предварительного ортогонального преобразования Уолша			
Гистограммы изображения при встраивании до сжатия JPEG, с проведением предварительного ортогонального преобразования В-К			

Таблица 3 – Деграция визуального качества изображения при встраивании

Пара бит 1 и 2	Пара бит 4 и 5	Тройка бит 1,2 и 3
		
$q(I') = \text{удовлетворительно}$	$q(I') = \text{неудовлетворительно}$	$q(I') = \text{неудовлетворительно}$
Визуальное качество изображения при встраивании после сжатия JPEG		
		
$q(I') = \text{хорошо}$	$q(I') = \text{удовлетворительно}$	$q(I') = \text{неудовлетворительно}$
Визуальное качество изображения при встраивании в процессе сжатия JPEG		
		
$q(I') = \text{хорошо}$	$q(I') = \text{удовлетворительно}$	$q(I') = \text{неудовлетворительно}$
Визуальное качество изображения при встраивании до сжатия JPEG, с проведением предварительного ДКП		
		
$q(I') = \text{отлично}$	$q(I') = \text{хорошо}$	$q(I') = \text{удовлетворительно}$
Визуальное качество изображения при встраивании до сжатия JPEG, с проведением предварительного ортогонального преобразования Уолша		
		
$q(I') = \text{отлично}$	$q(I') = \text{хорошо}$	$q(I') = \text{хорошо}$
Визуальное качество изображения при встраивании до сжатия JPEG, с проведением предварительного ортогонального преобразования В-К		

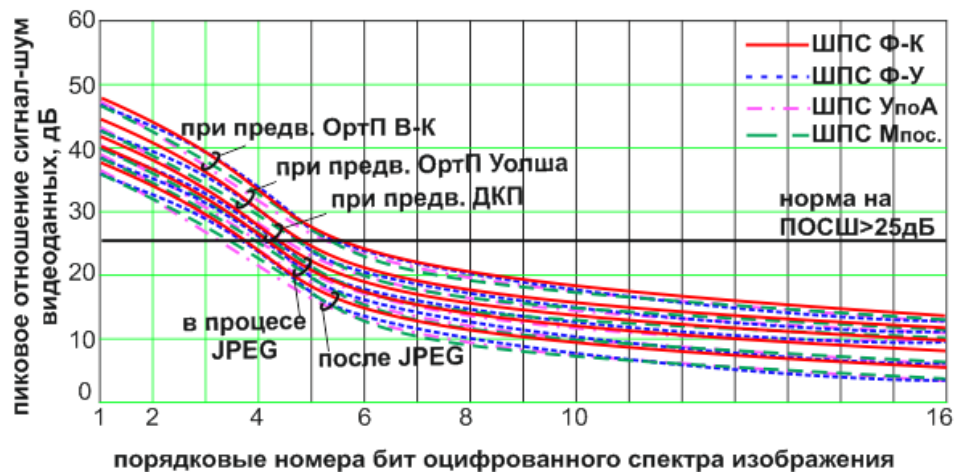


Рис. 2. Оценка пикового отношения сигнал шум для видеоданных после встраивания

При расчете всех параметров для оценивания скрытности встраивания рассмотрены все выбранные ДШСК в сочетании с разными вариантами порядка встраивания (после сжатия видеоданных, в процессе сжатия, до сжатия с проведением одного из ортогональных преобразований Уолша, В-К или ДКП) при модификации от одного до трех бит оцифрованного спектра.

Анализ гистограмм и субъективного оценивания визуального качества видеоданных позволяет сделать следующие выводы:

- 1) выбор вида ДШСК не оказывает значимого влияния на изменение гистограммы и визуального качества изображения, в отличие от выбора порядка встраивания уплотненного скрытого канала в видеоданные;
- 2) раздвоение пика гистограммы видеоданных, а также появление артефактов встраивания, проявляющихся в виде контрастных точек на изображении, после встраивания уплотненного скрытого канала наблюдаются лишь в случае встраивания в двоичный код значений яркости пикселей изображения после сжатия, что свидетельствуют о наименьшей скрытности такого подхода;
- 3) наименьших искажений гистограммы и визуального качества видеоданных позволяет достичь проведение предварительного ортогонального преобразования в базисе В-К,
- 4) встраивание более чем в пару бит приводит к значительным искажениям гистограммы и визуального качества видеоданных, таким образом, использование двух бит определяет максимально возможную пропускную способность уплотненного скрытого канала;
- 5) незначительные искажения гистограммы и визуального качества видеоданных получены при встраивании в номера парных бит оцифрованного спектра В-К видеоданных с первого по пятый, последующие пары бит значительно искажают гистограмму изображения, снижая скрытность встраивания уплотненных скрытых каналов.

Объективное оценивание скрытности встраивания по параметру пикового отношения сигнал шум свидетельствует о том, что лучших показателей позволяет достичь встраивание уплотненных скрытых каналов при проведении ортогональных преобразований Виленкина-Крестенсона видеоданных. При этом ограничение на качество встраивания в видеоданные по показателю пикового отношения сигнала-шум выполняется при модификации парных бит оцифрованного спектра В-К изображения не старше, чем четвертый и пятый. Таким образом, выполнение ограничений на скрытность встраивания возможно только в случае проведения предварительных двойных спектральных преобразований в базисе В-К видеоданных и модификации парных бит оцифрованного спектра с номерами до пятого включительно.

Алгоритмы кодового уплотнения, встраивания и извлечения данных скрытого канала из видеоданных

Для уточнения влияния ДШСК на выполнение ограничений на достоверность приема были разработаны новые алгоритмы кодового уплотнения, встраивания и извлечения данных уплотненного скрытого канала из видеоданных при их передаче [12] (рис. 3-5).

Разрабатываемый метод включает в себя как модель кодового уплотнения скрытого канала, так и новые алгоритмы:

- алгоритм уплотнения;
- алгоритмы встраивания и извлечения данных уплотненного скрытого канала из видеоданных.

Данные алгоритмы позволяют конкретизировать выводы, полученные в результате разработки модели, провести оценивание ограничений на достоверность приема скрываемых данных $S_k \in V, V = \{C_{скр}(S_k), p_{ош}(S'_k), k\}$ и расчет целевого показателя – числа ИНС СК при передаче видеоданных.

Новый оригинальный алгоритм кодового уплотнения отличается от известных способом разделения групп ИНС СК для последующего кодового уплотнения с использованием двумерных шумоподобных сигнальных конструкций Ф-К и представлен на рис. 3.

Разработанные новые алгоритмы встраивания и извлечения данных уплотненного скрытого канала отличаются от известных реализацией способа размещения до сжатия видеоданных и извлечения блочных конструкций Ф-К уплотненного скрытого канала в кадре видеоданных. Также элементом новизны является реализация этапа дополнительной обработки входных видеоданных путем проведения двумерных спектральных преобразований в базисе В-К с одновременной модификацией пары бит в оцифрованных значениях спектра видеоданных. Алгоритмы встраивания и извлечения данных уплотненного скрытого канала представлены на рис. 4-5. В ходе проведения исследований было проведено оценивание достоверности приема скрываемых данных (таблица 4). Установлено, что для обеспечения требуемого качества достоверности приема с учетом сжатия видеоданных только одновременное применение ДШСК Ф-К с согласованным ортогональным преобразованием В-К

позволяет соответствовать установленным требованиям, как по достоверности встраивания, так и по скрытности встраивания.

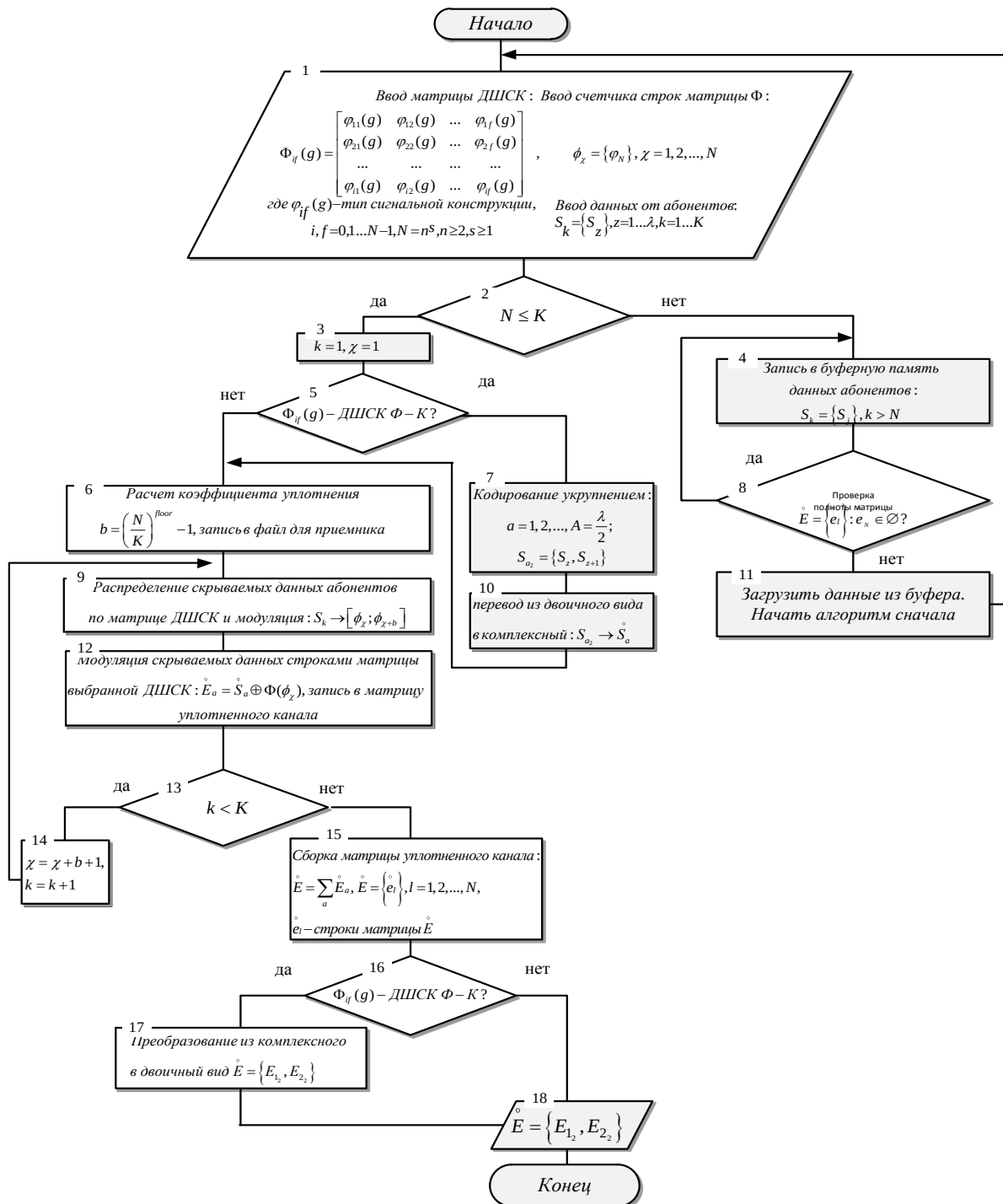


Рис. 3. Алгоритм кодового уплотнения скрытых каналов

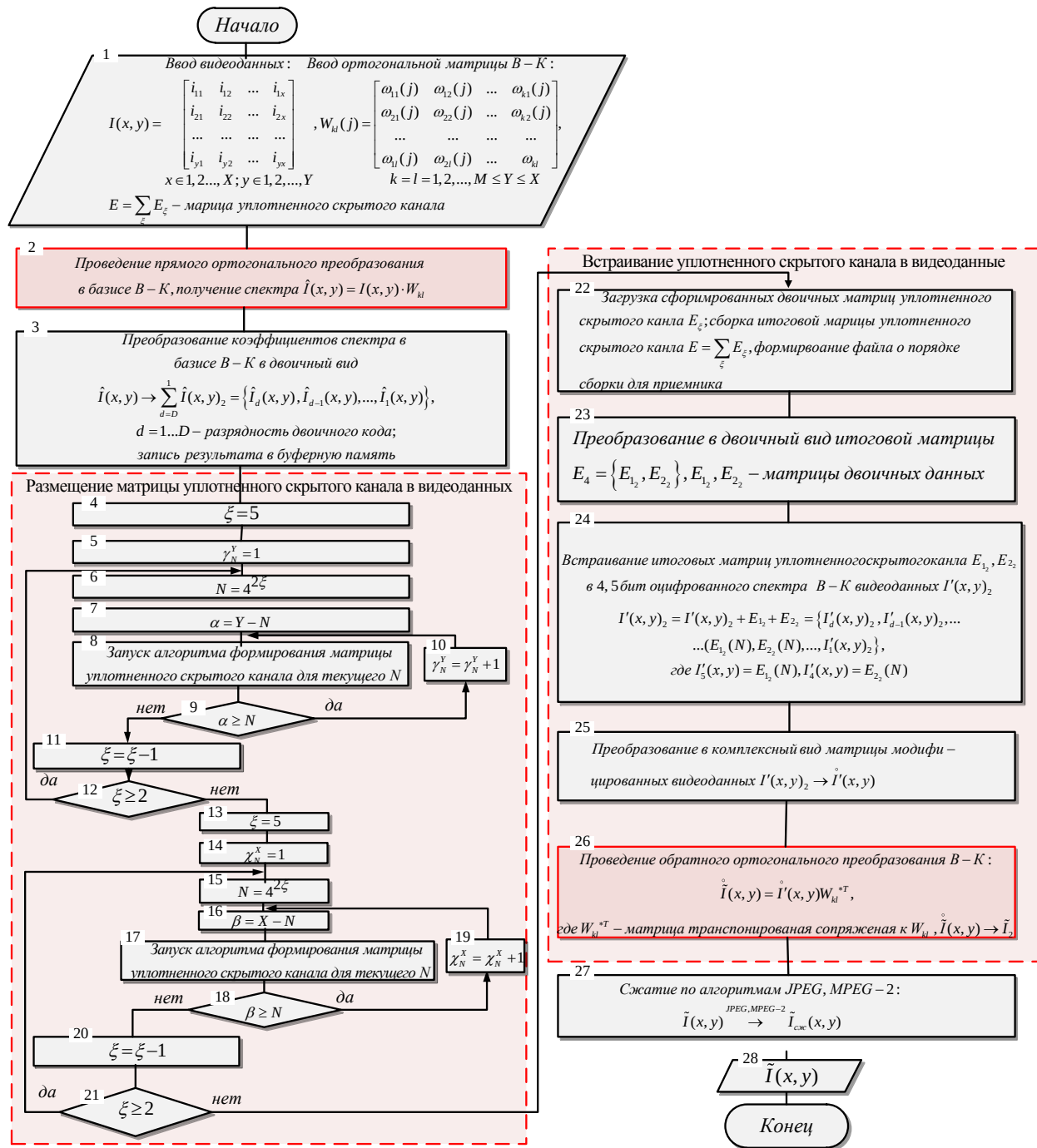


Рис. 4. Алгоритм встраивания уплотненных скрытых каналов в видеоданные

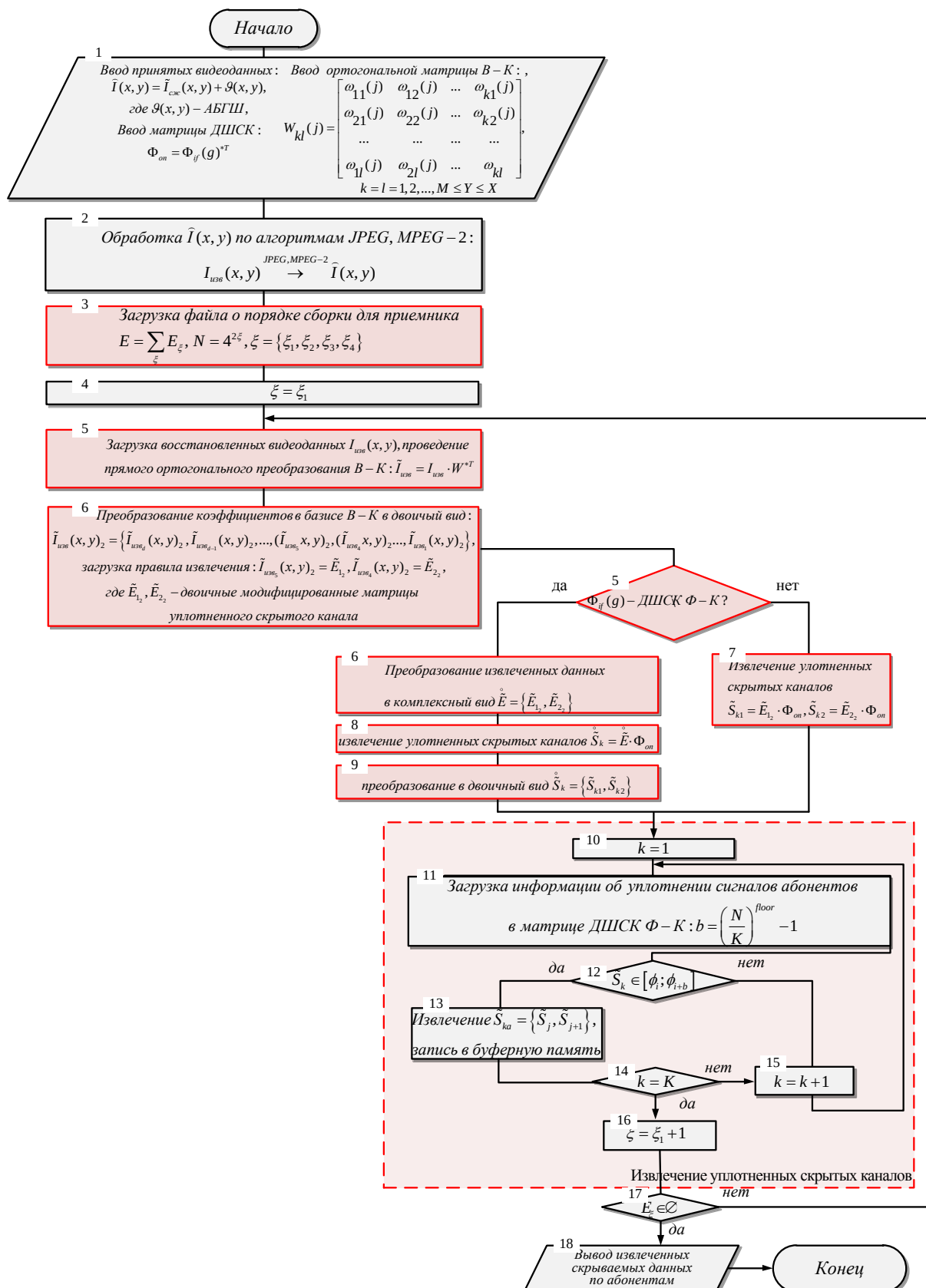


Рис. 5. Алгоритм извлечения уплотненных скрытых каналов из структуры видеоданных

Таблица 4 – Оценивание достоверности приема скрываемых данных

Сжатие в 2 раза		Сжатие в 100 раз	
1 Встраивание после сжатия JPEG при использовании ДШСК Ф-К			
2 Встраивание в процессе сжатия JPEG при использовании ДШСК Ф-К			
3.1 До сжатия JPEG, при проведении предварительного ДКП при использовании ДШСК Ф-К			
3.2 До сжатия JPEG, при проведении предварительного ортогонального преобразования Уолша при использовании ДШСК Ф-К			
3.3 До сжатия JPEG, при проведении предварительного ортогонального преобразования Виленикина-Крестенсона при использовании ДШСК Ф-К			

Анализ полученных графиков (таблица 4) свидетельствует о том, что наилучшими ДШСК, позволяющими выполнить требования по достоверности приема скрывааемых данных, являются ДШСК Ф-К. Учет условий, при которых выполнимы ограничения на скрытность встраивания, а именно: проведение двойных ортогональных преобразований в базисе В-К и модификации парных бит, не старше четвертого и пятого, а также сжатия видеоданных (не менее, чем в 100 раз) позволил уточнить одновременный выбор согласованной пары ДШСК Ф-К – ортогональное преобразование В-К для реализации метода кодового уплотнения скрытого канала при передаче видеоданных. Данный вывод подтверждается графиками представленными в таблице 4 для случая 3.3 при сжатии в 100 раз.

Расчет пропускной способности уплотненного скрытого канала

Для расчета пропускной способности уплотненного скрытого канала (рис. 6) и целевого показателя (рис. 7) – числа ИНС СК в видеопотоке были выведены формулы:

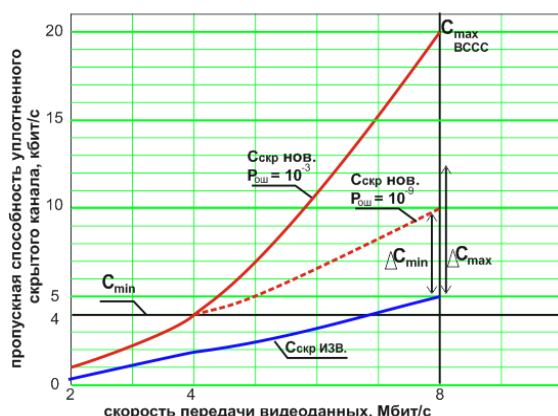
для видеоданных формата JPEG:

$$k_{скр} = \frac{C_{скр}}{k_{ед}} = \frac{\theta N_{осн} \cdot d \cdot \log_2 m}{k_{ед}},$$

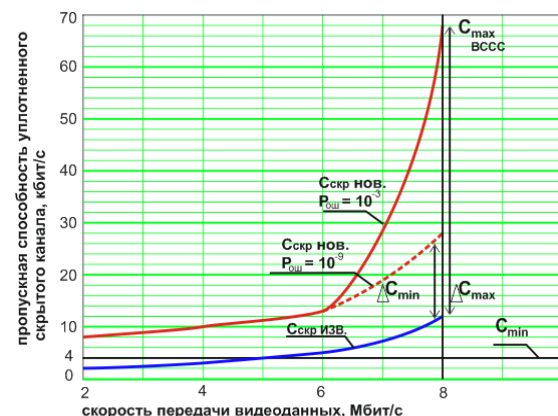
для видеоданных формата MPEG-2

$$k_{скр} = \frac{C_{скр}}{k_{ед}} = \frac{\theta N_{осн} d \cdot \log_2 m \cdot f}{G \cdot k_{ед}},$$

где $N_{осн} = m^{2^{\frac{f}{f_0}}}$ – период используемого ДШСК, $N_{осн} \leq X \leq Y$, $X \cdot Y$ – количество пикселей изображения-контейнера, размер изображения, θ – коэффициент вложения, определяющий число матриц уплотненных скрытых каналов максимального периода, d – число разрядов двоичного кода оцифрованного спектра изменяемых при встраивании (для разработанного метода – 2), m – значность используемых ДШСК (для ДШСК Ф-К – 4), f – частота кадров видео, G – размер группы кодирования видео, который определяет количество частоту следования основных кадров изображения (I-кадров), используемых для встраивания (для видео средней интенсивности – 12).

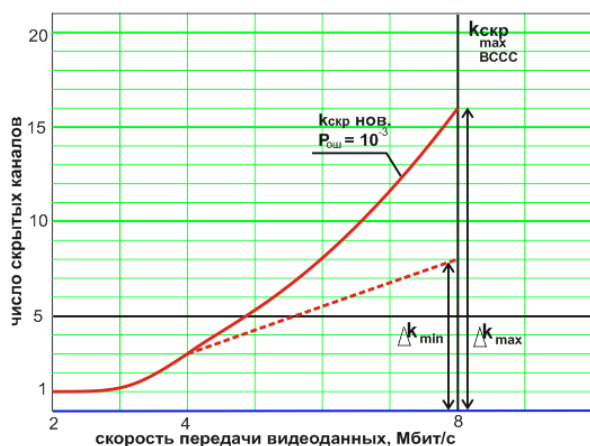


а) формат JPEG

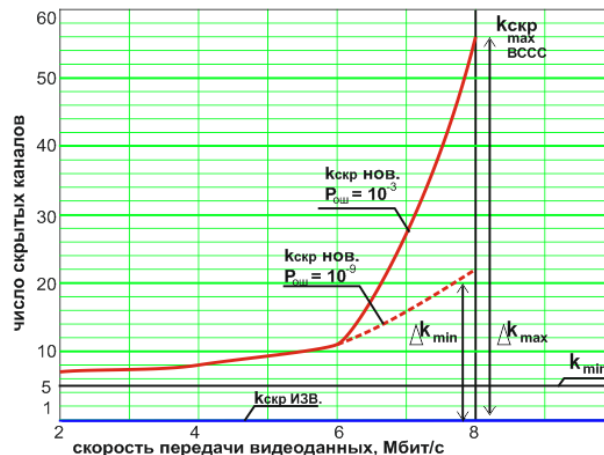


б) формат MPEG-2

Рис. 6. Зависимость пропускной способности уплотненного скрытого канала (бит/с) от скорости видеопотока (передача изображений)



а) формат JPEG



б) формат MPEG-2

Рис. 7. Зависимость числа ИНС СК в одном видеопотоке от скорости этого видеопотока

В соответствии с определенной в работе задачей минимально необходимое число ИНС СК в одном видеопотоке соответствует 5 каналам с общей пропускной способностью уплотненного канала – 4 кбит/с. Расчет числа ИНС СК в одном видеопотоке при организации скрытого обмена в видеоданных форматов JPEG, MPEG-2 представлен в таблице 5.

Таблица 5 – Расчет числа ИНС СК в одном видеопотоке при организации скрытого обмена в видеоданных форматах JPEG, MPEG-2

JPEG					MPEG-2				
Уровни качества	Низкий	Основной	Высокий		Уровни качества	Низкий	Основной	Высокий	
Размер кадра	352x288	720x576	1440x1150		Размер кадра	720x576	720x576	720x576	1440x1150
Скорость передачи	2 Мб/с	4 Мб/с	8 Мб/с		Частота смены кадров, Гц	25	30	40	40
Размещение матриц	1x256	4x256	20x256	1x1024+4x256	Скорость передачи	2 Мб/с	4 Мб/с	6 Мб/с	8 Мбит/с
Пропускная способность, кб/с	1,024	4,096	20,480	10,578	Размещение матриц	4x256	4x256	4x256	20x256
Число скрытых каналов	1	3	16	8	Пропускная способность, кб/с	8,53	10,2	13,65	68,27
Достоверность скрываемых данных, рош	10^{-3}	10^{-3}	10^{-3}	10^{-9}	Число скрытых каналов	7	8	11	56
					Достоверность скрываемых данных, рош	10^{-3}	10^{-3}	10^{-3}	10^{-9}

Таким образом, разработанный метод кодового уплотнения скрытого канала при передаче видеоданных позволяет организовать от 3 до 56 ИНС СК с пропускной способностью каждого ИНС СК 1,2 кбит/с и достоверностью 10^{-3} в зависимости от качества и формата видеоданных, используемых в качестве контейнера для встраивания.

Использование для встраивания видеоданных высокого качества (с размером кадра 1440×1150 и более) позволяет достичь лучших характеристик

достоверности передаваемых скрыто данных (10^{-9}) при уменьшении скрытой пропускной способности.

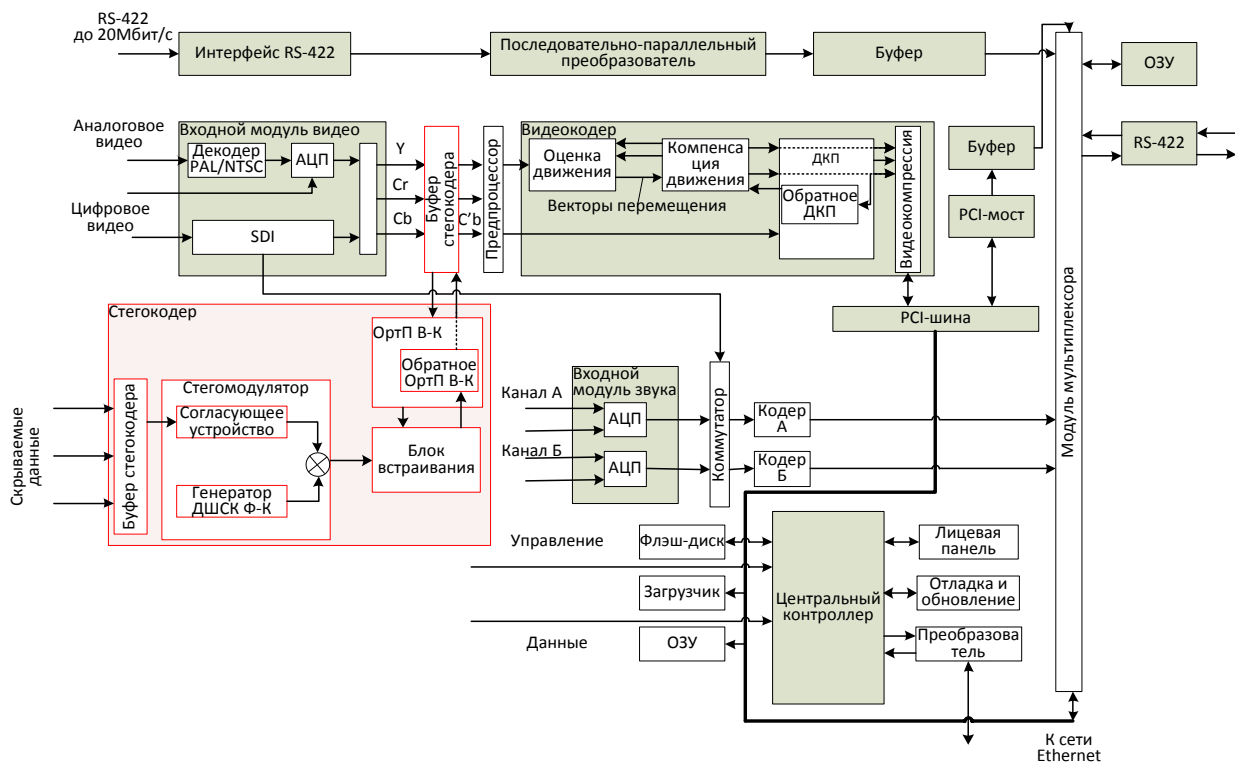
Предложения по совершенствованию типового кодера видеоданных

Предложения по совершенствованию типового кодера видеоданных представлены схмотехническими решениями (рис. 8). В работе определены тактико-технические характеристики кодера видеоданных с интегрированным стегокодером кодового уплотнения скрытого канала. Назначение усовершенствованного кодера видеоданных заключается в организации дополнительных ИНС СК в структуре открытого видеопотока при невозможности или нецелесообразности их передачи по открытым каналам связи. Основные требования, предъявляемые к входным видеоданным для организации уплотнения скрытого канала: видеоданные форматов JPEG или MPEG-2; количество неподвижных изображений, одновременно передаваемых за один сеанс связи – не менее 100, длительность видео трансляции – не менее 1 минуты.

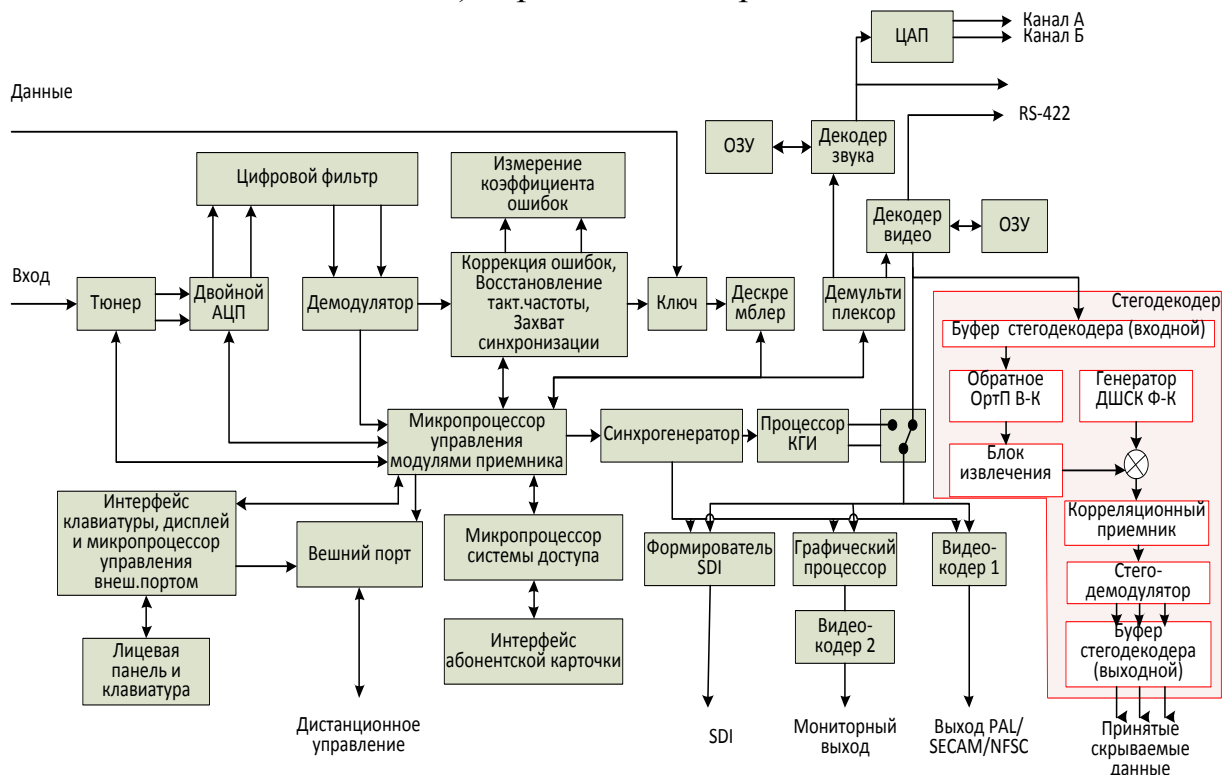
Возможности кодера видеоданных с интегрированным стегокодером для кодового уплотнения скрытого канала представлены в таблице 6.

Таблица 6 – Возможности кодера видеоданных с интегрированным стегокодером кодового уплотнения скрытого канала

Для входных видеоданных основного качества и основного профиля (размер кадра изображения 720x576)				
	2 Мб/с	4 Мбит/с	6 Мбит/с	8 Мбит/с
Вероятность ошибочного приема скрываемых данных 10^{-3}				
JPEG	1x1,024	1x4,096 / 3x1,2	1x10,1 / 8x1,2	1x13,4 / 11x1,2
MPEG-2	1x 8,5 / 7x1,2	1x10,2 / 8x1,2	1x16,4 / 13x1,2	1x20,1 / 16x1,2
Вид трафика, передаваемого по скрытым каналам – речь, телеграммы, электронная почта				
Для входных видеоданных высокого качества и основного профиля (размер кадра изображения 1140x1150)				
Скорость видеопотока - 8 Мбит/с				
Вероятность ошибочного приема скрываемых данных:				
	10^{-3}		10^{-9}	
JPEG	1x20,5 / 16 x1,2		1x10, 6 / 8x1.2	
MPEG-2	1x 68,3 / 56x1,2		1x27,3 / 22x1.2	



а) передающая сторона



б) приемная сторона

Рис. 8. Предложения по совершенствованию кодера видеоданных

Также были проведены расчеты вычислительной сложности разработанных алгоритмов кодового уплотнения, встраивания и извлечения ИН СК в структуру сжимаемых видеоданных, показавшие, что они могут быть реализованы на отечественных процессорах типа «Эльбрус».

Вывод

Научная новизна метода кодового уплотнения скрытого канала состоит в:

- разработке модели кодового уплотнения ИНС СК в видеоданных, отличающейся от известных проведением дополнительных этапов, состоящих как в реализации кодового уплотнения до сжатия видеоданных на основе двумерных шумоподобных сигнальных конструкций, так и проведением двойного ортогонального преобразования видеоданных с одновременным встраиванием согласованной с ним двумерной модулированной сигнальной конструкции;
- разработке алгоритма кодового уплотнения скрытого канала, отличающегося от известных алгоритмов способом разделения групп ИНС для последующего кодового уплотнения с использованием двумерных шумоподобных сигнальных конструкций Франка-Крестенсона, а также в разработке алгоритмов встраивания и извлечения данных из уплотненного скрытого канала, отличающиеся от известных алгоритмов реализацией способа размещения до сжатия видеоданных и извлечения блочных конструкций Франка-Крестенсона уплотненного скрытого канала в кадре видеоданных; реализацией этапа дополнительной обработки входных видеоданных путем проведения двумерных спектральных преобразований в базисе Виленкина-Крестенсона с одновременной модификацией пары бит в оцифрованных значениях спектра видеоданных.

Разработанный метод кодового уплотнения скрытого канала позволяет увеличить число ИНС СК в скрытом канале при передаче видеоданных при ограничениях на скрытность встраивания и достоверность приема скрываемых данных.

Литература

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002. – 272 с.
2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. – 283 с.
3. Абазина Е. С. Постановка задачи организации скрытого канала передачи информации с кодовым уплотнением в спутниковых радиоперелиниях для решения задач управления войсками // Сб. статей по материалам докладов Всероссийской науч.-практической конф. курсантов, слушателей и молодых ученых, посвященной Дню образования войск связи. Воронеж: ВУНЦ ВВС «ВВА». 2013. № 1. С. 385–388.
4. Абазина Е. С., Цветков К. Ю., Федосеев В. Е., Применение двумерных нелинейных сигналов Франка-Уолша, Франка-Крестенсона в методе формирования скрытых каналов с кодовым уплотнением в структуре сжимаемых видеоданных // Научные технологии в космических исследованиях Земли. 2013. № 4. С. 32–40.

5. Абазина Е. С. Выбор кодовых последовательностей для формирования широкополосных цифровых водяных знаков // Сборник материалов II Всероссийского конгресса молодых ученых (СПб, 20-22 марта 2013г.). – СПб., 2013. – С. 44–46.

6. Абазина Е. С. Метод скрытой передачи информации с кодовым уплотнением в видеоданных // Информация и космос. 2014. № 4. С. 33–38.

7. Абазина Е. С., Цветков К. Ю., Федосеев В. Е., Коровин В. М. Модель кодера скрытых каналов с кодовым уплотнением с использованием сигнальных последовательностей Франка–Уолша, Франка–Крестенсона // Труды НИИР. 2015. № 1. С. 1–11.

8. Абазина Е. С. Формирование стеганографического канала с кодовым уплотнением на основе двумерных нелинейных сигналов // Вопросы радиоэлектроники. Серия Техника телевидения. 2015. № 2. С. 111–118.

9. Цветков К. Ю., Федосеев В. Е., Коровин В. М., Абазина Е. С. Имитационная модель скрытой передачи информации с кодовым уплотнением в структуре сжимаемых видеоданных // Свидетельство о регистрации программы для ЭВМ № 2015615358, 2015.

10. Абазина Е. С. Математическая модель стегакодера для скрытого канала с кодовым уплотнением в структуре видеоданных // Проблемы эффективности и безопасности функционирования сложных технических и информационных систем: сб. материалов XXXII Всероссийской науч.-тех. конф.(Серпухов, 22 нояб. 2014г.). – Серпухов: МОУ ИИФ, 2014. – С. 17–21.

11. Абазина Е. С., Ерунов А. А. Результаты моделирования метода скрытой передачи информации с кодовым уплотнением в видеоданных // Системы управления, связи и безопасности. 2015. № 2. С. 1–25.

12. Абазина Е. С. Алгоритмы внедрения двумерных нелинейных кодовых последовательностей в видеопоток // Вопросы радиоэлектроники. Серия Техника телевидения. 2013. № 1. С. 85–93.

References

1. Gribunin V. G., Okov I. N., Turincev I. V. *Tsifrovaia steganografiia* [Digital Steganography]. Moscow, Solon-Press Publ, 2009. 272 p. (In Russian).

2. Konakhovich G. F., Puzirenko A. U. *Komputernaia steganografiia. Teoriia i praktika* [Computer steganography. Theory and practice]. Kiev, MK-Press Publ, 2006. 283 p. (In Russian).

3. Abazina E. S. Postanovka zadachi organizatsii skrytogo kanala peredachi informatsii s kodovym uplotneniem v sputnikovykh radioliniakh dlia resheniia zadach upravleniia voiskami [Statement of a problem of the organization of the hidden channel of information transfer with code consolidation in satellite radio lines for the decision of problems of management of armies]. *Materialy dokladov Vseros. nauchno-prakticheskoi konferentsii kursantov, slushatelei i molodykh uchenykh, posviashchennoi Dniu obrazovaniia voisk sviazi* [Day of Formation of Armies of Communication Proc. of the All-Russian Sci.-Pract. Conf. 32nd All-Russian Sci. and Tec. Conf.]. Voronezh, N. E. Zhukovsky and Y. A. Gagarin Military Air Academy Publ., 2013, no. 1, pp. 385 – 388 (In Russian).

4. Tsvetkov K. U., Fedoseev V. E., Abazina E. S. Primenenie dvumernih nelineinih signalov Franka-Uolsha, Franka-Krestensona v metode formirovaniya skritih kanalov s kodovim uplotneniem v structure szhimaemih videodannih [Application of two-dimensional nonlinear signals of Frank-Uolsh, Frank-Krestenson into the method of formation of the hidden channel with code consolidation in structure of the compressed video data]. *Hi-tech Earth Space Research*, 2013, no. 4, pp. 32–40 (In Russian).

5. Abazina E. S. Vybory kodovykh posledovatel'nostei dlia formirovaniia shirokopolosnykh tsifrovyykh vodianykh znakov. [Choice of code sequences for formation of broadband digital watermarks]. *II Mezhdvuzovskaya nauchno-prakticheskaya konferentsiya. Materialy dokladov* [Abstracts of Papers of 2nd All-Russian Congress of Young Scientists]. Saint-Petersburg, University of the Information's Technology, Mechanics and Optics Publ., 2013, pp. 44–46 (In Russian).

6. Abazina E. S. Metod skrytoi peredachi informatsii s kodovym uplotneniem v videodannykh [The method of hidden data transmission with code consolidation]. *Informatsiya i kosmos*, 2014, no. 4, pp. 33–38 (In Russian).

7. Tsvetkov K. U., Fedoseev V. E., Korovin V. M., Abazina E. S. Model kodera skritih kanalov s kodovym uplotneniem s ispolzovaniem signalnykh posledovatel'nostei Franka-Uolsha, Franka-Krestensona [Model of the coder of the hidden channel with code consolidation with use of signal sequences of Frank-Uolsh, Frank-Krestenson]. *Trudy NIIR*, 2015, no. 1, pp. 1–11 (In Russian).

8. Abazina E. S. Formirovaniye steganograficheskogo kanala s kodovym uplotneniem na osnove dvumernih nelineinih signalov [Forming of steganography data link with code consolidation, based on two-dimensional nonlinear signals]. *Voprosy radioelektroniki. Seriya tekhnika teledeniya*, 2015, no. 2, pp. 108–116 (In Russian).

9. Tsvetkov K. J., Fedoseyev V. E., Korovin V. M., Abazina E. S. *Imitatsionnaya model skrytoi peredachi informatsii s kodovym uplotneniem v structure szhimaemykh videodannykh. Svidetel'stvo o registratsii program dlya EVM* [Imitating model of the hidden information transfer with code consolidation in structure of the compressed video data. The Certificate on official registration of the computer program]. No. 2015615358, 2015.

10. Fedoseev V. E., Abazina E. S. Matematicheskaya model' stegokodera dlia skrytogo kanala s kodovym uplotneniem v structure videodannykh [Mathematical model of the stegocoder for the hidden channel with code consolidation in structure of the video data]. *Problemy effektivnosti i bezopasnosti funktsionirovaniya slozhnykh tekhnicheskikh i informatsionnykh sistem; Materialy XXXII Vseros. nauchno-tekhnicheskoi konferentsii* [Problems of Efficiency and Safety of Functioning Difficult Technical and Information Systems. Proc. 32nd All-Russian Sci. and Tec. Conf.]. Serpukhov, Serpukhov Military Rocket Institute Publ., 2014, pp. 17–21 (In Russian).

11. Abazina E. S. Rezultaty modelirovaniya metoda skrytoj peredachi informatsii s kodovym uplotneniem v videodannykh [Results of the modelling of the

method of the hidden information transfer with using of the code consolidation in the video data]. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 1-25 (In Russia).

12. Abazina E. S. Algoritmy vnedreniia dvumernykh nelineinykh kodovykh posledovatel'nostei v strukturu szhatykh videodannykh [Algorithms of introduction of two-dimensional nonlinear code sequences in structure of the compressed video data]. *Voprosy radioelektroniki. Seriya tekhnika televideniia*, 2013, no. 2, pp. 111–118 (In Russian).

Статья поступила 5 июля 2015 г.

Информация об авторе

Абазина Евгения Сергеевна – соискатель ученой степени кандидата технических наук. Адъюнкт кафедры Сетей и систем связи космических комплексов. Военно-космическая академия имени А. Ф Можайского. Область научных интересов: цифровая стеганография, теория приема и обработки сигналов, теория передачи информации. E-mail: e.s.abazina@yandex.ru

Адрес: 197198, Россия, г. Санкт-Петербург, Ждановская наб., д. 13.

Method of code consolidation of the hidden channel by transfer into video data

Abazina E. S.

Work urgency: increasing quantity of information directions of communication simultaneously functioning into hidden (steganographic) channel in structure of one multimedia container make questions of maintenance of applicability of methods digital steganography for wider class of problems more urgency. Known steganographic ways do not allow to organize hidden exchange more than one information direction of communication in a multimedia stream. The **work purpose** is to increase the number of information directions of communication in the hidden channel by transfer of the video data with restrictions on reliability of reception of the hidden data transferred in each information direction, and reserve of embedding. **Used methods:** it is offered to apply code consolidation of the data as the technology, allowing to reach the compromise in the contradiction between reserve of embedding, throughput of the hidden channel and reliability of reception of the hidden data. **Problem statement:** to develop a method of code consolidation of the hidden channels in structure of the video data. **Novelty:** novelty aspects of the presented decision are: carrying out of additional stages steganographic processings of the container and the built in data of each of the information directions of communication consisting as in realisation of code consolidation before compression of the video data with application two-dimensional noise-type of alarm designs, and carrying out of double orthogonal transformation of the video data with simultaneous embedding of the two-dimensional modulated alarm designs co-ordinated with it. Also it is necessary to carry a way of division of information directions of communication to a novelty aspect in the hidden channel, definition of the key data and an order of placing of the hidden data in an image-container shot. **Result:** Using developed method of code consolidation of the hidden channels in structure of the video data allows to increase number of information directions of communication in the hidden channel a minimum three times (at the hidden throughput of each information direction of communication of the hidden channel not less than 1.2 kbit/with and probabilities of erroneous reception of the hidden data are not worse 10^{-3}) and depends on a degree of quality of the video data. The maximum of the hidden throughput of the condensed hidden channel does not exceed 20 % from throughput of the channel of transfer of the video data. The **practical importance:** consists in finishing of the developed scientifically-methodical device and realised algorithms which allow to use results of researches by working out of the coder of the video data.

Keywords: *the video data, standards of compression JPEG, MPEG-2, стеганография, two-dimensional noise-type signal constructions, code consolidation (division) of the data.*

Information about Author

Abazina Evgeniya Sergeevna – Doctoral Student. The postgraduate student of the Department of Networks and Communication Systems of Space Complexes. Mozhaiskiy Military Space Academy. Field of research: digital steganography, the theory of signals. E-mail: e.s.abazina@yandex.ru

Address: Russia, 197198, Saint-Petersburg, Zhdanovskaya street, 13.

УДК 519.876

“Дорожные карты” с принятием решений на гибридных индикаторных сетях

Юдицкий С. А.

Актуальность. В настоящее время для принятия решений по достижению глобальных целей развития организационно-технических систем широкое распространение получили “дорожные карты”. Вместе с тем, в известных работах преобладает описательно-текстовый стиль изложения, следствием которого являются: неоднозначность модели, что вызывает трудности, в первую очередь, у предметных специалистов; ограничения при преобразованиях формальной составляющей дорожной карты. Указанные недостатки могут быть преодолены за счет применения сетевой дорожной карты на основе графо-логического описания – органического сочетания теории графов и математической логики (булевой алгебры). **Целью данной статьи** является разработка формальной сетевой графо-логической модели дорожной карты организационно-технической системы, отображающей динамику показателей (параметров) системы на заданном временном интервале. **Метод достижения цели**, предложенный в работе, заключается в разработке новой графо-логической модели организационно-технической системы, которую будем называть гибридной индикаторной сетью. **Новизна.** Отличительной особенностью гибридной индикаторной сети, по отношению к сети Петри, является измененный механизм срабатывания переходов, за счет введения дополнительного условия их срабатывания, определяемого введенными в модель индикаторными логическими функциями. **Результат.** Построение дорожной карты организационно-технической системы на основе предложенной гибридной индикаторной сети позволяет повысить ее выразительность и вариабельность (по сравнению со стандартными сетями Петри), за счет новой возможности изменения конфигурации графа путем применения индикаторных логических функций, определяющих условия срабатывания или блокировки переходов в сети. В статье дан пример построения гибридной индикаторной сети, и показано ее применение для анализа поведения организационно-технической системы.

Ключевые слова: дорожная карта, организационно-техническая система, сеть Петри, позиции и переходы, гибридная индикаторная сеть, графо-логическое описание, булева алгебра, индикаторная логическая функция.

Введение

Под дорожной картой применительно к организационно-техническим системам (ОТС) принято понимать комплект документации, определяющий последовательность работ по созданию новой ОТС и прогнозирование ее поведения. Эти работы частично выполняются по апробированным методикам, частично основываются на оригинальных решениях экспертов (экспертных семинаров). Масштабы и эффективность применения дорожных карт растут при увеличении степени формализации описания карт и совершенствования математического аппарата для моделирования функционирования ОТС в различных ситуациях. Вместе с тем, в известных автору работах по дорожным картам [1, 2, 3, 4] преобладает описательно-текстовый (неформальный) стиль изложения, следствием которого являются: неоднозначность в понимании модели; недостаточная наглядность и выразительность («непрозрачность») описания, что вызывает трудности, в первую очередь, у предметных специалистов; ограничения при преобразованиях формальной составляющей дорожной карты. Указанные недостатки могут быть преодолены (если не

полностью, то хотя бы частично) за счет применения сетевой дорожной карты на основе графо-логического описания – органического сочетания теории графов [5, 6] и математической логики (булевой алгебры [7, 8, 9]).

Целью данной статьи является разработка формальной сетевой графо-логической модели дорожной карты ОТС, отображающей динамику показателей (параметров) системы на заданном временном интервале.

Метод достижения цели, предложенный в статье, заключается во введении новой графо-логической модели ОТС, которую будем называть гибридной индикаторной сетью. Общим у такой сети и сети Петри [10, 11, 12], включая множество ее различных модификаций, является то, что в основе той и другой модели лежит двудольный граф. Вершины-позиции этого графа, изображаемые кружками, сопоставлены с переменными, принимающими численное или балльное значение. Вершины-переходы, изображаемые черточками или прямоугольниками, интерпретируются как события, изменяющие значения входных/выходных позиций перехода. Позиции соответствуют показателям ОТС (состояние системы и ее компонентов, ресурсы, внешние воздействия, реакции системы на протекающий в ней процесс, выпускаемая продукция и т.д.). Значения позиций могут сохраняться в течение нескольких тактов – промежутков между фиксированными моментами на временной шкале, переходы при возникновении соответствующих условий срабатывают мгновенно (в один и тот же момент).

Гибридная индикаторная сеть отличается от сети Петри как по форме описания, так и по механизму срабатывания переходов. Дуги графа, ведущие из входных позиций перехода в переход, помечаются так называемыми *индикаторными логическими функциями* [13, 14] (подробней будет разъяснено ниже). Если между переменными, соотнесенными вершинам графа, в данный момент имеют место заданные отношения (типа больше - меньше, равно и т.д.), то индикаторная функция, помечающая дугу, принимает единичное значение, и дуга активируется. В противном случае функция равна нулю, и дуга не активирована. Дуги графа, ведущие из перехода в выходные позиции, помечены логическими операторами, которые в момент срабатывания перехода присваивают выходным переменным заданные значения. Кроме того, переход нагружен булевой функцией, определенной на индикаторах всех входных дуг, и функцией, определяющей условия выбора выходных дуг при срабатывании перехода, если есть необходимость в таком выборе. Если переход «активирован по входу и детерминирован по выходу», и наступил какой-либо из фиксированных дискретных моментов на временной шкале, то переход срабатывает и изменяет значения переменных ОТС, находящихся под управлением логического оператора. Таким образом, происходит функционирование гибридной индикаторной сети, выполняющей роль дорожной карты ОТС. При этом в отличие от сетей Петри изменяются не только значения переменных, соотнесенных позициям сети, но может изменяться и конфигурация графа (при блокировании дуг). Гибридная

индикаторная сеть обладает большей выразительностью и вариабельностью, чем сеть Петри и ее модификации.

Построение гибридной индикаторной сети

Двудольный граф как статическая основа модели, задается в виде

$$G = \langle P, T, \alpha, \alpha^* \rangle,$$

где: $P = \{p_i, i=1, \dots, m\}$ – множество позиций графа, $T = \{t_i, i=1, \dots, n\}$ – множество переходов; $\alpha: T \rightarrow 2^P$, $\alpha^*: T \rightarrow 2^P$ – функции, задающие соответственно подмножества входных и выходных позиций перехода; 2^P – множество всех подмножеств P . Пример двудольного графа, заимствованный из [11], дан на рис 1, внешние переменные (имеют только выходные дуги) обозначены через x_1, x_2 , внутренние переменные (имеют входные и выходные дуги) – через $p_1, \dots, p_4$.

Индикатором сравнения будем называть булеву переменную вида

$$z = (y_1 \# y_2),$$

где y_1, y_2 – переменные, одна из которых может быть константой, $\#$ – знак бинарного отношения, выражаемого множеством $\{=, \neq, >, \geq, <, \leq\}$. Индикатор принимает значение $z=1$, если выполняется отношение $\#$, и $z=0$, если не выполняется. Описание индикатора выделяется скобками. Формальное выражение, полученное путем применения конечное число раз к индикаторам сравнения логических операций конъюнкции ($\wedge$), дизъюнкции ($\vee$), отрицания (черта сверху), также является индикаторной формулой, принимающей значения 1 или 0.

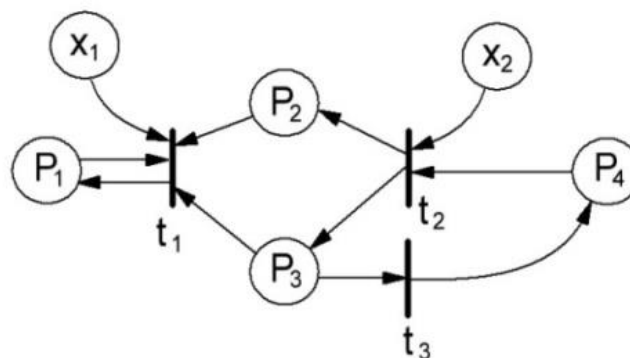


Рис 1. Пример двудольного графа

Сопоставление дугам двудольного графа индикаторных формул. Дуги графа будем выражать упорядоченной парой, состоящей из символа позиции и символа перехода, где левый символ соответствует началу дуги, а правый – ее концу. Индикаторные функции, помечающие дуги, обозначим через $\Phi_j(\bullet)$, $j=1, \dots, k$ – порядковый номер дуги графа.

Для графа на рис. 1 примем следующий набор индикаторных функций с аргументами-позициями, определенными на 10-балльной шкале:

$$\begin{aligned}\Phi_1(x_1 t_1) &= (x_1 > 0) \wedge (x_1 \leq 10); \\ \Phi_2(p_1 t_1) &= ((p_1 > 1) \wedge (p_1 < 4)) \vee ((p_2 \geq 4) \wedge (p_3 \geq 4)); \\ \Phi_3(p_2 t_1) &= (p_2 \leq 3) \wedge (p_1 < 6); \\ \Phi_4(p_3 t_1) &= (p_3 < 4) \wedge (p_2 < 6); \\ \Phi_5(t_1 p_1) &= (p_1 > 2) \wedge ((p_2 > 5) \vee (p_3 > 5)); \\ \Phi_6(x_2 t_2) &= (x_2 > 0) \wedge (x_2 \leq 10); \\ \Phi_7(p_4 t_2) &= (p_4 < 8) \wedge (x_2 > 2); \\ \Phi_8(t_2 p_2) &= (p_2 < 5); \\ \Phi_9(t_2 p_3) &= (p_3 < 5); \\ \Phi_{10}(p_3 t_3) &= (p_3 \geq 3); \\ \Phi_{11}(t_3 p_4) &= (p_4 \geq 4).\end{aligned}$$

Индикаторные логические формулы переходов. Для каждого перехода t графа составляется индикаторная логическая формула, отображающая его динамику и результат срабатывания:

$$F(t) = L[\Phi(\tau)] \rightarrow O[P(\tau/\tau+1)],$$

в которой приняты следующие обозначения: F - продукция (нотация ЕСЛИ-ТО, изображенная горизонтальной стрелкой); $L[\Phi]$ - логическая функция над индикаторами из множества Φ (пометками дуг) в момент τ , $O[\bullet]$ - логический оператор изменения значений позиций из множества P при смене момента τ на момент $\tau+1$. В рассматриваемом примере имеем формулы:

$$\begin{aligned}F(t_1) &= ((\Phi_2 \wedge \Phi_3) \vee (\Phi_1 \wedge \Phi_4)) \rightarrow (p_1(\tau+1) = p_1(\tau) + 1); \\ F(t_2) &= (\Phi_6 \wedge \Phi_7) \rightarrow (p_2(\tau+1) = p_2(\tau) + 1) \wedge (p_3(\tau+1) = p_3(\tau) + 1); \\ F(t_3) &= \Phi_{10} \rightarrow (p_4(\tau+1) = p_4(\tau) + 2).\end{aligned}$$

Вышеприведенное формальное описание пометок дуг Φ и механизма срабатывания переходов F дает алгебраическое представление гибридной индикаторной сети.

Моделирование гибридных индикаторных сетей

Результатом моделирования гибридной индикаторной сети является последовательность упорядоченных наборов значений переменных, сопоставленных внутренним позициям сети, на дискретной временной шкале $\tau = 0, 1, \dots, N$. Считаются заданными начальные условия - значение внешних и внутренних позиций в момент $\tau=0$, набор целевых значений внутренних переменных и нормативная продолжительность эксперимента моделирования, выраженная числом тактов. Результат моделирования считается успешным, если за время, не превосходящее нормативное, достигнут целевой набор, причем в ходе процесса имитации ни одна внутренняя переменная не вышла за пределы 10-балльного интервала (0 - 10).

Рассмотрим алгоритм моделирования динамики гибридной индикаторной сети на примере, описанном приведенными в предыдущем разделе системами уравнений типа Φ и типа F . Описание будем иллюстрировать таблицей 1.

Таблица 1 - Моделирование гибридной индикаторной сети

τ	0	1	2	3	4	5	6	7	8	9	10
t		$t_1 t_2 t_3$	t_3	t_3	$t_1 t_2 t_3$	$t_1 t_2 t_3$	$t_1 t_3$	t_3	$t_1 t_3$	t_3	t_3
X_1	0	3	3	5	1	2	0	0	0	0	0
X_2	0	0	0	2	4	5	0	0	0	0	0
P_1	0	0	1	1	1	2	3	4	4	5	5
P_2	0	0	1	1	1	2	3	3	3	3	3
P_3	3	3	4	4	4	5	6	6	6	6	6
P_4	0	0	2	4	6	8	10	12	14	16	18
Φ_1	0	1	1	1	1	1	0	0	0	0	0
Φ_2	0	0	0	0	0	1	1	0	1	0	0
Φ_3	1	1	0	1	1	1	1	0	1	1	1
Φ_4	1	1	0	0	0	0	0	0	0	0	0
Φ_5	0	0	0	0	0	0	1	1	1	1	1
Φ_6	0	0	0	1	1	1	0	0	0	0	0
Φ_7	0	0	0	0	1	0	0	0	0	0	0
Φ_8	1	1	1	1	1	1	1	1	1	1	0
Φ_9	1	1	1	1	1	0	0	0	0	0	0
Φ_{10}	1	1	1	1	1	1	1	1	1	1	1
Φ_{11}	0	0	0	1	1	1	1	1	1	1	1

В верхней строке таблицы дана временная шкала, где столбцы соответствуют тактам, а вертикальная линия – левая граница столбца соотнесена дискретному моменту τ . Во 2-ю сверху строку вписываются определенные при моделировании переходы, инициирующие наступление данного такта. Далее (при движении сверху вниз) следует сектор X внешних переменных. Они, также как внутренние переменные, измеряются в 10-балльной системе счисления, но моменты их изменения не определены и носят случайный характер. Следующий сектор P соответствует внутренним переменным, а под ним располагается сектор Φ , в который вносятся логические значения 1 или 0, характеризующие пометки дуг. Заполнение таблицы производится по тактам, в направлении слева направо.

Алгоритм моделирования гибридной индикаторной сети работает следующим образом. В начальном такте $\tau=0$ система находится в равновесном состоянии, когда не активирован ни один переход (левая клетка строки t пуста). Вывести систему из равновесия может только изменение значения внешних переменных. В любом такте τ , где $(\tau > 0) \wedge (\tau \leq N)$, причем предыдущий такт $\tau-1$ характеризовался срабатыванием переходов (соответствующая клетка в столбце $\tau-1$ не пуста), выполняется последовательность действий:

- 1) Изменяются значения внешних переменных в секторе X согласно реальной ситуации;
- 2) Изменяются значения внутренних переменных из сектора P , инициированные логическими операторами вследствие срабатывания переходов в предыдущем такте $\tau-1$ (см. приведенную в предыдущем разделе статьи систему уравнений типа F , отображающих причинно-

- следственную связь между логическими условиями и логическими операторами в модели гибридной индикаторной сети);
- 3) Значения всех внешних и внутренних переменных, как измененных, так и неизмененных, переносим из столбца $\tau-1$ в столбец τ ;
 - 4) В столбце τ в секторе Φ вычисляем логические значения всех функций Φ_j по данным выше уравнениям на основе значений внешних и внутренних переменных в этом столбце;
 - 5) По результатам п. 4 на основе системы уравнений из предыдущего раздела статьи определяем переходы, активизированные в такте τ , и заносим их в клетку во 2-й строке столбца τ .

Примечание. Предложенная модель в отличие от сети Петри разрешает одновременное срабатывание нескольких переходов. Во избежание противоречий между значениями выходных позиций этих переходов, применяются условия корректности (ограничения на модель), которые здесь не рассматриваются.

Проиллюстрируем действия алгоритма на примере столбца $\tau=2$, для которого в предыдущем столбце были активированы все переходы. В секторе X значения внешних переменных x_1, x_2 были перенесены без изменения из предыдущего столбца. В секторе P под воздействием логических операторов значение внутренних переменных p_1, p_2, p_3 увеличено на 1, а переменной p_4 на 2. В секторе Φ значения функций Φ_j пересчитаны в соответствии с новыми значениями аргументов. Из переходов в соответствии с формулами «логическое условие – оператор» активирован только переход t_3 .

Результатом моделирования, отображенном в таблице 1, является динамика внутренних переменных $p_1, \dots, p_4$ на временном интервале (горизонте) $\tau = 0, 1, \dots, 10$. Переменные p_1, p_2, p_3 находятся в допустимом диапазоне, переменная p_4 в такте $\tau=7$ выходит за верхнюю границу значения внутренней переменной при моделировании и далее продолжает расти.

Заключение

В работе, в рамках методологии дорожных карт [13, 14], предложены гибридные индикаторные сети как формальный инструмент для предварительного имитационного моделирования и анализа поведения создаваемых сложных систем различного назначения, в том числе организационно-технических систем.

Все большее распространение в мире получает точка зрения, согласно которой развертыванию больших, сложных и дорогостоящих проектов должно предшествовать создание группы моделей. Первичными в этой группе являются, несомненно, компьютерные модели, позволяющие лучше понять предложенную идею, принципы функционирования и управления задуманной системой, ее конкурентные преимущества. Это дает виртуальный базовый запас знаний, на основе которого уже можно приступить к созданию фрагментарных материальных, организационных и иных моделей, расширяющих и углубляющих упомянутый запас знаний. И, наконец, выйти на генеральную

комплексную (компьютерно-материально-организационную) модель как основу проекта системы. В такой комплексной стратегии гибридные индикаторные сети оказываются на одном из начальных мест в цепочке создания новых эффективных систем в различных предметных областях. Вместе с тем, как можно судить по литературе, теория дорожных карт только начинает формироваться (по крайней мере, в России). Автор предлагает читателю очень скромную работу на эту тему, надеясь вместе с тем на возможность ее дальнейшего полезного развития.

При имитационном моделировании на основе гибридных индикаторных сетей может быть выявлен ряд угроз [15], устранение которых на этапе рабочего проектирования, а тем более апробации и эксплуатации, обойдется значительно дороже, а при эксплуатации вообще чревато поломкой, аварией и даже катастрофой. Примеры угроз: помимо проиллюстрированного выше выхода параметров за допустимые пределы, «зависание» (блокирование) работы системы при недостаточности ресурсов, заикливание – повторение некоторой последовательности состояний системы неограниченное число раз, недопустимое превышение запланированных сроков создания системы, и т.д.

Литература

1. Кузык Ю. Что такое дорожная карта // Наука и технологии России - STRF.ru, 18.05.2009. URL: http://www.strf.ru/material.aspx?CatalogId=223&d_no=20108#.VavbJrXQRW9 (дата обращения 12.07.2015).
2. Джемала М. Корпоративная «дорожная карта» // Российский журнал менеджмента. 2008. Т. 6. № 4.
3. Карасев О. И. Методология разработки технологических дорожных карт. – М.: ИСИЭЗ, 2009. URL: <http://www.slideshare.net/ssuser7c02b4/karasev> (дата обращения 12.07.2015).
4. Лидин К. Л. Многообразие построения дорожных карт, 2006. URL: <http://pandia.ru/text/77/396/40434.php> (дата обращения 12.07.2015).
5. Зыков А. А. Основы теории графов. – М.: Наука, 1987. – 384 с.
6. Харари Ф. Теория графов. – М.: Мир, 1973. – 301 с.
7. Гильберт Д., Аккерман В. Основы теоретической логики / пер. с нем. Ерофеева А. А. – М.: Государственное издательство Иностранной литературы, 1947. – 304 с.
8. Клини С. К. Математическая логика. – М.: Мир, 1973. – 480 с.
9. Кузнецов О. П. Дискретная математика для инженера. – СПб: Лань, 2007. – 400 с.
10. Котов В. Е. Сети Петри. – М.: Наука, 1984. – 160 с.
11. Питерсон Д. Теория сетей Петри и моделирование систем. – М.: Мир, 1984. – 264 с.
12. Юдицкий С. А., Магергут В. З. Логическое управление дискретными процессами. – М.: Машиностроение, 1987. – 176 с.
13. Юдицкий С. А. Моделирование динамики многоагентных триадных сетей. – М.: Синтег, 2012. – 112 с.

14. Юдицкий С. А. Триадно-сетевые дорожные карты развития систем // Управление большими системами, 2013, № 42.
15. Дернер Д. Логика неудачи. – М.: Смысл, 1997. – 243 с.

References

1. Kuzyk Iu. What is road map. *Science and technologies of Russia STRF.ru*, 18.05.2009. Available at: http://www.strf.ru/material.aspx?CatalogId=223&d_no=20108#.VavbJrXQRW9 (accessed 12 July 2015) (in Russian).
2. Jemala M. Corporate Roadmapping. The Innovative Tool of Corporate Knowledge Management. *Russian Management Journal*, 2008, vol. 6, no. 4 (in Russia).
3. Karasev O. I. *Metodologiya razrabotki tekhnologicheskikh dorozhnykh kart* [Methodology Development of Technology Roadmaps]. Moscow, Institute for Statistical Studies and Economics of Knowledge, 2009. Available at: http://www.strf.ru/material.aspx?CatalogId=223&d_no=20108#.VavbJrXQRW9 (accessed 12 July 2015) (in Russian).
4. Lidin K. L. *Mnogoobrazie postroeniia dorozhnykh kart* [The Diversity of the Construction of Roadmaps], 2006. Available at: <http://pandia.ru/text/77/396/40434.php> (accessed 12 July 2015) (in Russian).
5. Zykov A. A. *Osnovy teorii grafov* [The Basics of Graph Theory]. Moscow, Nauka Publ., 1987. 384 p. (in Russian).
6. Kharari F. *Teoriia grafov* [Graph Theory]. Moscow, Mir Publ., 1973. 301 p. (in Russian).
7. Hilbert D., Ackermann W. *Grundzuge Der Theoretischen Logik* [Principles of theoretical logic]. New York, 1946.
8. Klini S. K. *Matematicheskaya logika* [Mathematical Logic]. Moscow, Mir Publ., 1973. 480 p (in Russian).
9. Kuznetsov O. P. *Diskretnaya matematika dlia inzhenera* [Discrete Mathematics for Engineer]. St. Petersburg, Lan' Publ, 2007. 400 p. (in Russian).
10. Kotov V. E. *Seti Petri* [Petri Nets]. Moscow, Nauka Publ, 1984, pp. 11-58 (in Russian).
11. Peterson James L. *Petri net theory and the modeling of systems*. The University of Texas at Austin, 1981.
12. Iuditskii S. A., Magergut V. Z. *Logicheskoe upravlenie diskretnymi protsessami* [Logical Control of Discrete Processes]. Moscow, Mashinostroenie Publ., 1987 (in Russian).
13. Iuditskii S. A. *Modelirovanie dinamiki mnogoagentnykh triadnykh setei* [Modeling the Dynamics of Multi-Agent Triadic Nets]. Moscow, Sinteg Publ., 2012 (in Russian).
14. Iuditskii S. A. The triadic-networked roadmaps for systems development. *Large-scale Systems Control*, 2013, vol. 42 (in Russian).
15. Derner D. *Logika neudachi* [The logic of failure]. Moscow, Smysl Publ., 1997. 243 p. (in Russian).

Статья поступила 11 июля 2015 г.

Информация об авторе

Юдицкий Семен Абрамович - доктор технических наук, профессор, главный научный сотрудник. Институт проблем управления им. В.А. Трапезникова. Область научных интересов: моделирование организационно-технических систем. Тел. +7 495 339 59 10. E-mail: yuseab32@yandex.ru

Адрес: Россия, 117997, Москва ул. Профсоюзная, д. 65.

“Road Map” with Decision-Making by Hybrid Indicated Net

Iuditskii S. A.

Problem statement: Currently the “road map” has been widely disseminated for decision-making for achieving the global objectives of development of organizational and technical systems. However, the descriptive text style prevails in the majority of works. The consequences of this presentation are: the ambiguity models; constraints in the transformation of the formal component of the roadmap. These drawbacks can be overcome through the use of road network maps based on the graph of the logic description is an organic combination of graph theory and mathematical logic (Boolean algebra). **Purpose:** the development of a formal net graph-logic model roadmap of organizational-technical system that displays the dynamics of indicators (parameters) of the system at a given time interval. **Methods:** creation of new graph-logical models of organizational and technical systems, which we will call hybrid flat network. **Novelty.** Hybrid indicated net distinguish from Petri nets by mechanism of triggering of transitions, by introducing additional conditions for their operation, as defined entered in the model indicator logical functions. **Results** “road map” of organizational-technical system is built based on the hybrid indicated net more expressive and varied (compared to standard Petri nets). In a hybrid indicated net configuration of graph is changed by applying a logical indicator function, determining the conditions for triggering or blocking of transitions in the net. The author cites the example of construction and application of hybrid indicated net to analyze the behavior of organizational and technical systems.

Key words: road map, organizational-technical system, Petri nets, position and transition, Hybrid indicated net, graph-logic description, Boolean algebra, indicator-logical function.

Information about Author

Iuditskii Semen Abramovich - Dr. habil. of Engineering Sciences, Full Professor, Senior Research Officer of Institute of Control Sciences RAS. Field of research: modeling of organizational and technical systems. Tel.: +7 495 339 59 10. E-mail: yuseab32@yandex.ru

Address: Russia, 117997, Moscow, Profsoyuznaya str., 65.

УДК 004.724.4

Модели и алгоритмы маршрутизации в транспортной наземно-космической сети связи военного назначения

Михайлов Р. Л.

Постановка задачи: применение современных технологий организации пакетных сетей передачи данных в транспортных наземно-космических сетях связи военного назначения актуализирует вопросы обеспечения устойчивости их функционирования, оказывающей существенное влияние на своевременность информационного обмена в системах управления войсками и оружием. Показано, что известные протоколы маршрутизации не обеспечивают требуемый уровень устойчивости связи в условиях целенаправленного воздействия внешних деструктивных факторов и, следовательно, существует необходимость их усовершенствования. **Целью работы** является повышение устойчивости транспортных наземно-космических сетей связи военного назначения путем разработки моделей и алгоритмов маршрутизации информационных потоков в условиях целенаправленного воздействия внешних деструктивных факторов. **Используемые методы:** в работе нашли применение методы теории вероятности, теории надежности, теории марковских случайных процессов и теории графов. **Новизной** работы является введение показателя устойчивости связи, учитывающего зависимость между эффектом от воздействия внешних деструктивных факторов в виде отказа каналов связи и параметрами сетевого уровня эталонной модели взаимодействия открытых систем, а также критерий выбора временных параметров сигнализации в целях повышения этого показателя. **Результат:** проведенное моделирование показало, что использование разработанных алгоритмов позволяет обеспечить требуемый уровень устойчивости наземно-космических сетей связи военного назначения, при этом эффективность их использования по выбранному в работе показателю достигает 80%. **Практическая значимость** работы заключается в доведении разработанного научно-методического аппарата до программной модификации протокола маршрутизации PNNI для математического обеспечения коммутатора пакетов

Ключевые слова: система спутниковой связи, транспортная сеть связи, устойчивость связи, маршрутизация, ATM, PNNI.

Актуальность

В настоящее время в Вооруженных Силах Российской Федерации (ВС РФ) определены основные задачи и направления развития системы военной связи (СВС) ВС РФ. Особенности построения транспортной сети СВС ВС РФ являются использование в ее составе каналов связи (КС) космического эшелона в качестве резерва при невозможности передачи данных через инфраструктуру наземного эшелона и, следовательно, ее функционирование на основе технологий, используемых в военных системах спутниковой связи (ВССС). Вместе с тем, принципы и основные технологические решения современных ВССС были разработаны до 1995 года и не в полной мере отвечают современным требованиям, предъявляемым в ВС РФ. Имеется серьезное технологическое отставание ВССС от аналогов ведущих зарубежных стран, в первую очередь, по пропускной способности и видам предоставляемых услуг. Одним из основных технологических направлений совершенствования ВССС является внедрение современных сетевых телекоммуникационных технологий в состав перспективных космических аппаратов связи (КАС) и оборудования земных станций (ЗС). В качестве

технологического решения по обеспечению коммутации пакетов и каналов в ВССС впервые предполагается использование АТМ-маршрутизатора, позволяющего реализовать функции как коммутации пакетов, так и функции коммутатора цифровых каналов для передачи абонентского трафика. Однако внедрение современных технологий построения транспортных сетей связи наряду с неоспоримыми преимуществами влечет за собой появление дополнительных уязвимостей СВС ВС РФ, связанных с функционированием в условиях целенаправленных дестабилизирующих воздействий. Одной из характеристик информационного обмена в системе управления войсками и оружием (СУВО) является своевременность передачи трафика, зависящая, в том числе, от устойчивости СВС ВС РФ. Вместе с тем, снижение устойчивости основы СВС ВС РФ, а именно транспортной наземно-космической сети связи (ТНКСС), в условиях, когда применение средств огневого поражения против КАС и ЗС маловероятно, связано с воздействием средств радиоэлектронного противоборства (РЭП) [1]. В этих условиях протокол маршрутизации PNNI (Private Network-to-Network Interface – частный межсетевой интерфейс), входящий в состав стека АТМ (Asynchronous Transfer Mode – асинхронный метод передачи) не сможет обеспечить выполнение требований по своевременности информационного обмена, предъявляемых к СВС ВС РФ.

Вопросы маршрутизации рассмотрены в работах Ададунова С.Е., Бертсекаса Д., Вишневого В.М., Дейкстры Э.В., Косякова Е.Н., Назарова А.И., Новикова С.Н., Сычева К.И. Методическим аспектам оценивания и повышения устойчивости связи посвящены работы Боговика А.В., Гречишникова Е.В., Дадонова А.Г., Игнатова В.В., Исакова Е.Е., Кучерявого А.Е., Ландэ Д.В., Нетеса В.А., Стекольников В.Ю., Попкова В.К., при этом в более узкой области помехозащищенности (радиоэлектронного противоборства) исследования проводились Антоновичем П.И., Борисовым В.И., Владимировым В.И., Зинчуком В.М., Комаровичем В.Ф., Коцыняком М.А., Куприяновым А.И., Липатниковым В.А., Стародубцевым Ю.И., Чудновым А.М. Задача разработки элементов научно-методического аппарата повышения устойчивости связи на сетевом уровне эталонной модели взаимодействия открытых систем (ЭМВОС) нашла свое отражение в работах Бабусенко С.И., Бутова А.А. и Паршуткина А.В., при этом специфика ТНКСС СВС ВС РФ, связанная с технологическими решениями в области спутниковой связи, не учитывалась.

Таким образом, работа преследует достижение актуальной цели, состоящей в повышении устойчивости ТНКСС СВС ВС РФ в условиях воздействия средств РЭП.

Постановка задачи

В течение продолжительного промежутка времени под устойчивостью связи понималась совокупность трех свойств: надежности, живучести и помехоустойчивости [2]. Авторы монографии [2] указывали, что применение интегральной категории устойчивости не предполагает ликвидации составляющих ее понятий. При этом надежность отражает влияние на

работоспособность системы главным образом внутрисистемного фактора – случайных отказов техники, а живучесть же характеризует устойчивость системы связи против действия причин, лежащих вне системы и приводящих к разрушениям или значительным повреждениям некоторой части ее элементов. Подчеркивалось, что надежность и живучесть – существенно различные понятия и самостоятельные проблемы, требующие своих решений при разработке и совершенствовании систем и сетей связи [3].

В работе [4], авторами давалось следующее определение: «Устойчивость – способность сети сохранять работоспособное состояние во времени и в условиях, создаваемых воздействиями внешних и внутренних деструктивных факторов (ДФ). При этом пояснялось, что устойчивость характеризуется свойствами надежности и живучести. Далее указывалось, что свойство надежности должно обеспечивать функционирование сети связи и ее элементов в условиях действия внутренних непреднамеренных (случайных) ДФ, а живучесть – свойство сети сохранять способность выполнять требуемые функции в условиях, создаваемых воздействием внешних ДФ [4].

В работе [5] приводятся определения понятий устойчивости, целостности и безопасности единой сети связи (СС), используемых в законах «О техническом регулировании» (2002 г.) и «О связи» (2003 г.). В частности, в ней дается следующее определение: «Устойчивость функционирования единой сети электросвязи – свойство сети связи выполнять свои функции при воздействии внешних дестабилизирующих факторов».

В настоящее время требования к устойчивости функционирования сетей электросвязи, входящих в состав сети связи общего пользования, и методы их проверки установлены в ГОСТ 5311-2008 [6]. В данном нормативном документе приведены следующие основные определения.

Устойчивость функционирования сети электросвязи – способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате воздействия дестабилизирующих факторов [6].

Дестабилизирующий фактор – воздействие на сеть электросвязи, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети электросвязи характера, приводящее к выходу из строя элементов сети [6].

Коэффициент готовности – вероятность того, что объект находится в работоспособном состоянии в любой момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается [6].

Надежность сети электросвязи – свойство сети электросвязи сохранять способность выполнять требуемые функции в условиях воздействия внутренних дестабилизирующих факторов (т. е. сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения и технического обслуживания) [6].

Внутренний дестабилизирующий фактор – дестабилизирующий фактор, источник которого расположен внутри сети электросвязи или ее элементов [6].

Живучесть сети электросвязи – свойство сети электросвязи сохранять способность выполнять требуемые функции в условиях, создаваемых воздействиями внешних дестабилизирующих факторов [6].

Внешний дестабилизирующих факторов – дестабилизирующий фактор, источник которого расположен вне сети электросвязи [6].

Работоспособное состояние – состояние объекта, при котором значения всех параметров, характеризующих способность выполнять им свои функции, соответствует требованиям или нормам [6].

Среднее время между отказами – отношение суммарной наработки восстанавливаемого объекта к математическому ожиданию числа его отказов в течение этой наработки [6].

Направление связи (основное направление связи) – совокупность линий передачи и узлов связи, обеспечивающая связь между двумя пунктами сети для обеспечения деятельности органов государственного управления, обороны, безопасности, охраны правопорядка, мобилизационной готовности при чрезвычайных ситуациях [6].

Вероятность связности (связность) направления электросвязи – вероятность того, что на заданном направлении электросвязи существует хотя бы один путь, по которому возможна передача информации с требуемым качеством и объемом [6].

Граф сети связи – математическая модель сети электросвязи, представляющая собой совокупность вершин (узлов связи) и соединяющих их ребер (линий связи) [6].

Элемент (объект) сети электросвязи – отображаемые на графе сети электросвязи вершинами и ребрами узлы связи и соединяющие их линии (совокупность линий) связи [6].

Вместе с тем, как показано в работе [7], устойчивость связи, являясь одним из основных свойств СВС, характеризуется некоторыми терминологическими отличиями в ходе своей оценке. Так, в соответствии с руководящими документами, в качестве внешних ДФ рассматриваются отдельно обычное и ядерное оружие противника, а также естественные и преднамеренные помехи. Специфика оценки устойчивости систем военной связи включает в себя:

Живучесть – способность СВС обеспечивать управление войсками, силами и оружием в условиях воздействия обычного и ядерного оружия противника.

Помехоустойчивость – способность СВС обеспечивать управление войсками, силами и оружием в условиях воздействия естественных помех.

Помехозащищенность – способность СВС обеспечивать управление войсками, силами и оружием в условиях воздействия преднамеренных помех противника.

Надежность – способность СВС обеспечивать связь, сохраняя во времени значения эксплуатационных показателей в пределах, соответствующих условиям эксплуатации, технического обслуживания восстановления и ремонта.

В работе [8] показано место устойчивости СВС в общей системе управления войсками и оружием (рис. 1).

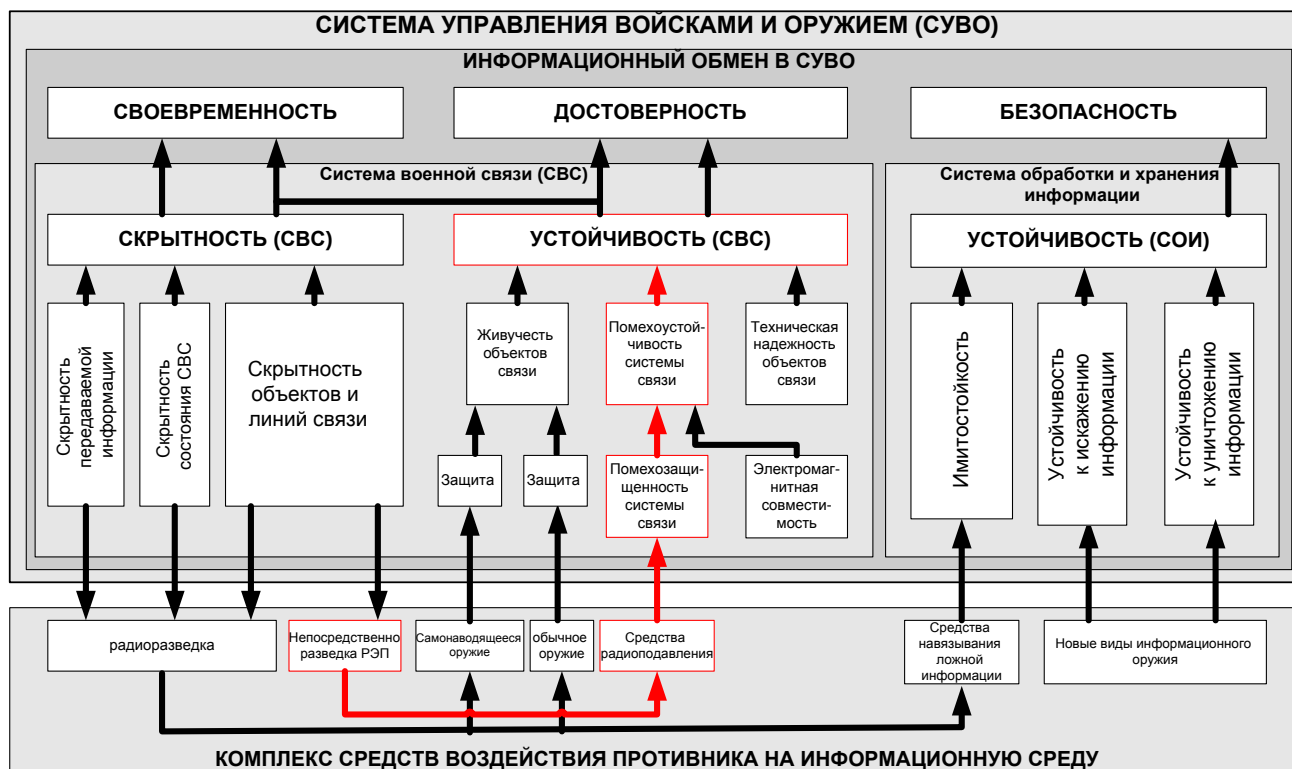


Рис. 1. Место устойчивости СВС в системе управления войсками и оружием

В работе [7] на основе анализа действующего в настоящее время ГОСТа [6], а также исследований других авторов показано, что показателем устойчивости связи является значение вероятности связности информационного направления связи (ИНС) $P_{св}$, под которым понимается вероятность того, что на заданном направлении существует хотя бы один путь, по которому возможна передача информации с требуемым качеством (QoS) и объемом:

$$P_{св} = P(k_{QoS} \geq 1 \mid \{Q_k\} \in \{Q_{\text{треб}}\}), \quad (1)$$

где k_{QoS} – количество работоспособных путей на заданном ИНС, обеспечивающих заданное качество обслуживания QoS; Q_k – качество обслуживания, обеспечиваемое путями (путем) на заданном ИНС; $Q_{\text{треб}}$ – требуемый уровень качества обслуживания.

Кроме того, в работах [7, 9, 10] для характеристики устойчивости ТНКСС СВС ВС РФ предложен показатель вероятности своевременной доставки пакета, проведен анализ методик расчета этого показателя для транспортных СС, осуществляющих передачу информационного трафика в соответствии с технологией АТМ, и предложено следующее аналитическое выражение:

$$P_{\text{сд}} = P_{\text{пр}} K_{\Gamma} P_{\text{св}} \left| T_{\text{дост}} \leq T_{\text{дост}}^{\text{зад}} \right., \quad (2)$$

где $P_{\text{пр}}$ – вероятность безошибочной доставки пакета, $P_{\text{св}}$ – вероятность связности ИНС, K_{Γ} – коэффициент готовности ИНС, $T_{\text{дост}}^{\text{зад}}$ – заданное значение максимального времени доставки пакета.

Вероятность безошибочной доставки пакета $P_{\text{пр}}$ определяется способностью применяемой системы помехоустойчивого кодирования обнаруживать и исправлять ошибки, возникающие при приеме информационного пакета. В рамках работы сделано допущение о том, что ошибки, возникающие при приеме пакета, будут обнаруживаться и исправляться с помощью системы помехоустойчивого кодирования в полном объеме, т.е. $P_{\text{пр}}=1$.

В соответствии с выражением (2) вероятность связности ИНС $P_{\text{св}}$ служит для описания способности структуры СС обеспечить связность графа, ее формализующего, в условиях исключения отдельных ребер (подавления отдельных КС) или вершин (приведение в неработоспособное состояние узлов связи) [7]. Кроме того, значение вероятности связности ИНС $P_{\text{св}}$ зависит от типа ИНС, построенного в СС используемым протоколом маршрутизации. Так, в случае если ИНС представляет собой последовательное соединение элементов (рис. 2), то, применяя известные выражения из теории надежности, получим вероятность связности ИНС $P_{\text{св}1}$, с учетом вероятности работоспособного состояния отдельных элементов $P_{\text{раб.эл.}v}$ [11]:

$$P_{\text{св}1} = \prod_{v=1}^{z_1} P_{\text{раб.эл.}v}. \quad (3)$$

Под элементом соединения понимается канал или узел связи, имеющий собственные значения устойчивости к воздействию внешних и внутренних ДФ, определяемых показателем вероятности работоспособного состояния $P_{\text{раб.эл.}v}$ в соответствии с методикой [7].

$$P_{\text{раб.эл.}v} = (1 - P_{\text{ИТВ}v})(1 - P_{\text{РЭП}v})(1 - P_{\text{ФП}v})(1 - P_{\text{отк}v}), \quad (4)$$

где $P_{\text{ИТВ}i}$ – вероятность отказа элементов ИНС вследствие информационно-технических воздействий (ИТВ) [12]; $P_{\text{РЭП}i}$ – вероятность отказа вследствие воздействия средств РЭП количества КС в ИНС большего, либо равного величине реберной связности графа, формализующего ИНС; $P_{\text{ФП}i}$ – вероятность физического поражения узлов связи ИНС большего, либо равного величине вершинной связности графа, формализующего ИНС; $P_{\text{отк}i}$ – вероятность отказа элементов ИНС вследствие воздействия внутренних ДФ и естественных процессов надежности.

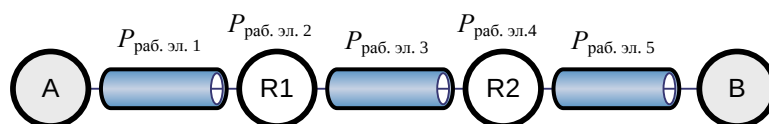


Рис. 2 ИНС с последовательным соединением элементов

В случае независимости элементов и возможности осуществлять резервирование путей, ИНС имеет вид, представленный на рис. 3.

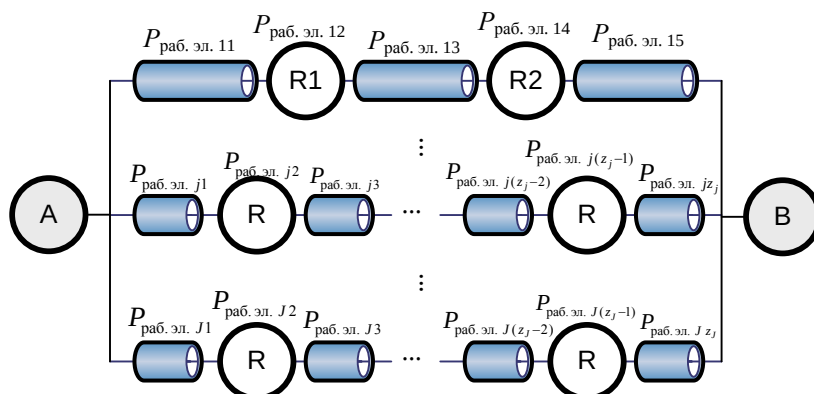


Рис. 3 ИНС с параллельно-последовательным соединением элементов

В случае независимости элементов путей в ИНС и отсутствии пересечений, применяя известные выражения из теории надежности, получим суммарную вероятность связности для такой структуры ИНС $P_{св\ 2}$ [11]:

$$P_{св\ 2} = 1 - \prod_{j=1}^J \left(1 - \prod_{v=1}^{z_j} P_{раб.\ эл.\ v} \right). \quad (5)$$

В случае смешанной структуры путей, в том числе при наличии их пересечений, получим структуру, представленную на рис. 4. Для такой структуры путей в составе ИНС применяется его разбиение на отдельные последовательно объединенные области, с последующим вычислением вероятности связности $P_{св}$ сначала внутри такой области, затем в целом за ИНС.

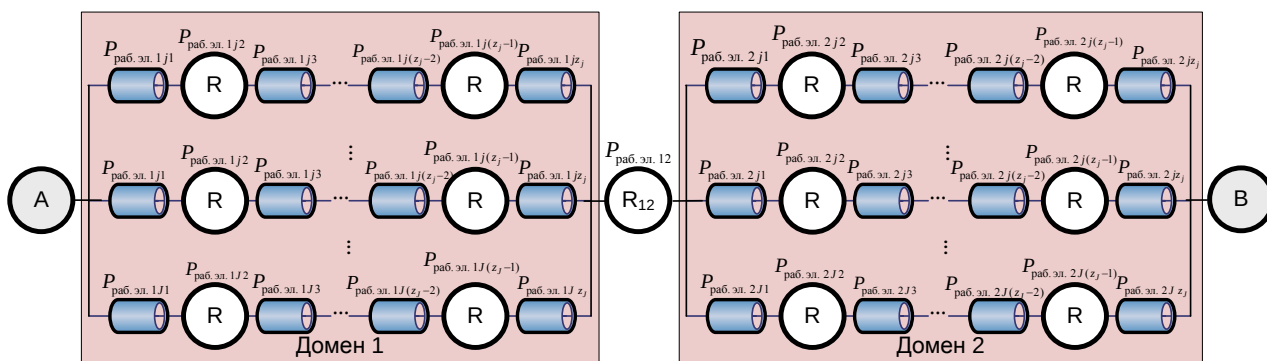


Рис. 4 ИНС со смешанной структурой

На практике вид, представленный на рис. 4, имеют ИНС, используемые протоколами PNNI в сетях MPLS (ATM, ASON, IP-MPLS), разбитых на

множество доменов маршрутизации. При этом каждая область соответствует отдельному домену, а маршрутизаторы, в которых пересекаются пути, соответствуют граничным маршрутизаторам. Дополнительные пути в каждом домене для схем соединений на рис. 3 и рис. 4 соответствуют принципу резервирования соединений 1+1 или 1:1 [13].

На основе известных выражений из теории надежности с учетом выражений (4) и (5), получим суммарную вероятность связности для такой структуры ИНС $P_{св3}$:

$$P_{св3} = \prod_{i=1}^d \left(1 - \prod_{j=1}^{J_i} \left(1 - \prod_{v=1}^{z_j} P_{\text{раб. эл. } v} \right) \right) \cdot \prod_{i=1}^{d-1} P_{\text{раб. эл. } v}, \quad (6)$$

где первая часть произведения определяет вероятность связности доменов, а вторая – вероятность связности граничных маршрутизаторов.

Существенную роль в определении вероятности своевременной доставки пакета $P_{сд}$ играют временные параметры функционирования ИНС и его реакции на отказ элементов, определяемые коэффициентом готовности ИНС K_{Γ} . Выражение для коэффициента готовности ИНС должно определять не только долю времени работоспособного состояния ИНС при отказе его отдельных элементов с учетом времени на восстановление элементов, но и время реакции протокола сигнализации на диагностику отказа и восстановление связи (или реконфигурацию). Кроме того, для современных протоколов маршрутизации само понятие отказа КС несколько отличается от принятого. Протоколы реагируют не только на полную утерю работоспособности элементом, но и на частичное понижение его характеристик, приводящее к превышению времени доставки пакета заданного значения $T_{\text{дост}}^{\text{зад}}$. Таким образом, особенности функционирования СС на сетевом уровне ЭМВОС при маршрутизации информационных потоков проявляются в форме зависимости значения коэффициента готовности ИНС K_{Γ} от временных интервалов сигнализации и временных параметров отказов КС:

$$K_{\Gamma} = F(T_{\text{диагн}}, T_{\text{ож}}, T_{\text{рек}}, T_{\text{отк КС}}), \quad (7)$$

где $T_{\text{отк КС}}$ – среднее время работы между отказами КС, $T_{\text{диагн}}$ – время диагностики отказа ИНС; $T_{\text{ож}}$ – время ожидания восстановления связи в ИНС, $T_{\text{рек}}$ – время реконфигурации путей в ИНС.

С учетом вышесказанного, вербально задача работы формулируется как повышение устойчивости ТНКСС СВС ВС РФ по показателю вероятности своевременной доставки пакета $P_{сд}$ за счет разработки НМА маршрутизации информационных потоков, позволяющих повысить коэффициент готовности ИНС. В математическом виде задача формализуется следующим образом.

Дано:

$$P_{\text{сд}} = P_{\text{пр}} K_{\Gamma} P_{\text{св}} \Big| T_{\text{дост}} \leq T_{\text{дост}}^{\text{зад}},$$

$$E_y = \left(\frac{P_{\text{сд}2}}{P_{\text{сд}1}} - 1 \right) \times 100\% = \left(\frac{K_{\Gamma 2}}{K_{\Gamma 1}} - 1 \right) \times 100\%,$$

$$K_{\Gamma} = F(T_{\text{диагн}}, T_{\text{ож}}, T_{\text{рек}}, T_{\text{отк КС}}),$$

$$P_{\text{сд}}^{\text{зад}} = 0,9 \Big| T_{\text{дост}}^{\text{зад}} = 3 \text{ с.}$$

Найти:

$$(T_{\text{диагн}}, T_{\text{ож}}, T_{\text{рек}}) \left\{ \begin{array}{l} P_{\text{сд}} \geq P_{\text{сд}}^{\text{зад}} \Big| T_{\text{дост}}^{\text{зад}} \leq 3 \text{ с.} \\ E_y \rightarrow \max \end{array} \right. , \quad (8)$$

где $P_{\text{сд}}$ – вероятность своевременной доставки пакета, $T_{\text{дост}}$ – максимальное время доставки пакета, $T_{\text{дост}}^{\text{зад}}$ – заданное значение максимального времени доставки пакета, $P_{\text{сд}1}$ – вероятность своевременной доставки пакета без использования разработанных алгоритмов, $P_{\text{сд}2}$ – вероятность своевременной доставки пакета с использованием разработанных алгоритмов, $P_{\text{св}}$ – вероятность связности ИНС, $P_{\text{пр}}$ – вероятность безошибочной доставки пакета; K_{Γ} – коэффициент готовности ИНС, $K_{\Gamma 1}$ – коэффициент готовности ИНС без использования разработанных алгоритмов, $K_{\Gamma 2}$ – коэффициент готовности ИНС с использованием разработанных алгоритмов, E_y – показатель эффективности использования разработанных алгоритмов, $T_{\text{отк КС}}$ – среднее время между отказами КС, $T_{\text{диагн}}$ – время диагностики отказа ИНС; $T_{\text{ож}}$ – время ожидания восстановления связи в ИНС, $T_{\text{рек}}$ – время реконфигурации путей в ИНС.

Показатель эффективности использования разработанных алгоритмов E_y отражает прирост значения коэффициент готовности ИНС K_{Γ} вследствие использования разработанных элементов НМА маршрутизации информационных потоков.

Для достижения поставленной цели в работе решаются следующие задачи.

- 1) Разработка модели функционирования АТМ-маршрутизатора при изменении метрики каналов связи вследствие воздействия средств РЭП.
- 2) Разработка модели функционирования межузлового соединения ТНКСС в условиях воздействия средств РЭП.
- 3) Разработка алгоритма маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС.
- 4) Разработка алгоритма адаптивного изменения временных параметров сигнализации в межузловом соединении ТНКСС в условиях воздействия средств РЭП.

Модель функционирования АТМ-маршрутизатора при изменении метрики каналов связи вследствие воздействия средств РЭП

В рамках разработанной модели оценено влияние изменения сигнально-помеховой обстановки на канальные и сетевые показатели КС в условиях использования адаптивных схем выбора вида модуляции сигнала и скорости помехоустойчивого кодирования в каналах спутниковой связи DVB-S2.

Особенностью реализации протокола DVB-S2 для каналов спутниковой связи является наличие режима ACM (Adaptive Coding and Modulation) для адаптивного выбора вида сигнала и скорости кодирования в зависимости от отношения сигнала к шуму и помехе (ОСШП) на входе приемника. Это позволяет осуществлять гибкое регулирование параметрами кодирования и модуляции передатчика в зависимости от значения ОСШП на входе приемника при заданном уровне достоверности приема. При этом параметры кодирования и модуляции могут изменяться от кадра к кадру. В стандарте DVB-S2 предусматриваются следующие скорости кодирования FEC (1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9 и 9/10) при ёмких видах модуляции (QPSK, 8-PSK, 16-APSK и 32-APSK). Для защиты от ошибок приема сигналов в стандарте DVB-S2 используется перемежение данных и наложение двухуровневого кода для прямой коррекции ошибок FEC. В качестве внутреннего кода используется код LDPC, в качестве внешнего – код БЧХ (код Боуза-Чоудхури-Хоквенгема). Таким образом, благодаря возможности адаптивного выбора вида модуляции и скоростей кодирования каналы могут работать в широком диапазоне значений ОСШП с показателем спектральной эффективности, близким к теоретически достижимому. Так, канал связи DVB-S2, может работать при ОСШП от -2,4 дБ (модуляция QPSK, скорость кода $R=1/4$) до 16 дБ (модуляция 32-APSK, скорость кода $R=9/10$), при этом для этого канала доступны показатели эффективности спектра от 0,5 до 4,5 (бит/с)/Гц. Схемы адаптивного выбора вида модуляции и скорости кодирования для DVB-S2 приведены в таблице 1 по данным, представленным в работах [14-19].

В работах [20, 21] показано, что отображением развития радиоэлектронного конфликта на параметры канала связи является периодическое изменение его пропускной способности. Для формализованного описания периодического изменения пропускной способности канала связи в работах [20, 21] предложено использовать зависимость показателя отношения сигнал к сумме шум и помеха формализованную выражением:

$$q(t) = \left[\begin{array}{l} F_1(q_{\min}, F_s, P_j, \gamma, t_{\text{сск}}, t_{\text{РП}}, t) \\ F_2(q_{\min}, F_s, L, w_{ji}, \varphi_{ji}, t_{\text{сск}}, t_{\text{РП}}, t) \end{array} \right] P_E = P_{E \max} \quad (9)$$

где $q_{\min}$ – значение ОСШП в КС, при котором невозможна передача информации; F_s – полоса частот СРС; P_j – мощность помехи; γ – коэффициент, характеризующий часть полосы частот ВРС, занимаемую помехой $0 \leq \gamma \leq 1$; P_E – средняя вероятность ошибки на бит; L – число немодулированных гармонических колебаний; w_{ji} и φ_{ji} – частота и начальная фаза i -го

гармонического колебания; $t_{скз}$ – время, необходимое для смены сигнально кодовых созвездий; $t_{рп}$ – время реакции помех.

В качестве канальных показателей рассматривались пропускная способность и время задержки при передаче. В качестве сетевых показателей рассматривались метрика КС, а также метрика виртуальных путей (VPC – Virtual Path Connect), создаваемых протоколом PNNI в магистральных спутниковых каналах. В качестве воздействия средств РЭП рассматривалась наихудшая помеха, определяемая по показателю средней вероятности ошибки на бит. Под отказом КС понимается ухудшение ОСШП вследствие воздействия средств РЭП ниже заданной в технологии DVB-S2 критической величины ($q_{min} = -2,35$ дБ), при котором еще обеспечивается достоверный прием сигнала. При отказе VPC суммарная метрика КС, входящих в его состав, не позволяет осуществлять передачу пакетов с заданным уровнем времени задержки.

Схема взаимосвязи аналитических соотношений в модели функционирования маршрутизатора в условиях изменения метрики каналов связи вследствие воздействия средств РЭП представлена на рис. 5. Более подробно указанная модель, а также исследования на ее основе приведены в работах [22].

Анализ результатов моделирования позволяет сделать следующие выводы.

- 1) Изменение ОСШП напрямую влияет на изменение параметров сетевого уровня – метрик КС и метрик VPC.
- 2) Отказы отдельных КС и VPC, характеризующиеся средним временем между отказами КС $T_{отк\ КС}$ и VPC $T_{отк\ VPC}$ соответственно, приводят к отказу соединения АТМ, при этом суммарный поток отказов (рис. 6) характеризуется плотностью вероятности распределения времени между отказами соединения АТМ $f^*(T_{отк\ АТМ})$, которая может быть аппроксимирована экспоненциальной зависимостью (рис. 7).
- 3) При рассмотрении наиболее вероятных классов помех в качестве воздействия средств РЭП, наибольшее влияние на количественные параметры суммарного потока отказов соединения АТМ будут оказывать отказы КС.

Экспоненциальная зависимость плотности вероятности распределения времени между отказами соединения АТМ $f^*(T_{отк\ АТМ})$ и тот факт, что данные отказы вызваны, в первую очередь, отказами КС, позволили сделать допущение о пуассоновском процессе отказов соединения АТМ вследствие воздействия средств РЭП, при условии ординарности отказов КС. Данное допущение позволяет обосновать переход от соотношения временных интервалов сигнализации к вероятностным параметрам марковской модели межузлового соединения ТНКСС.

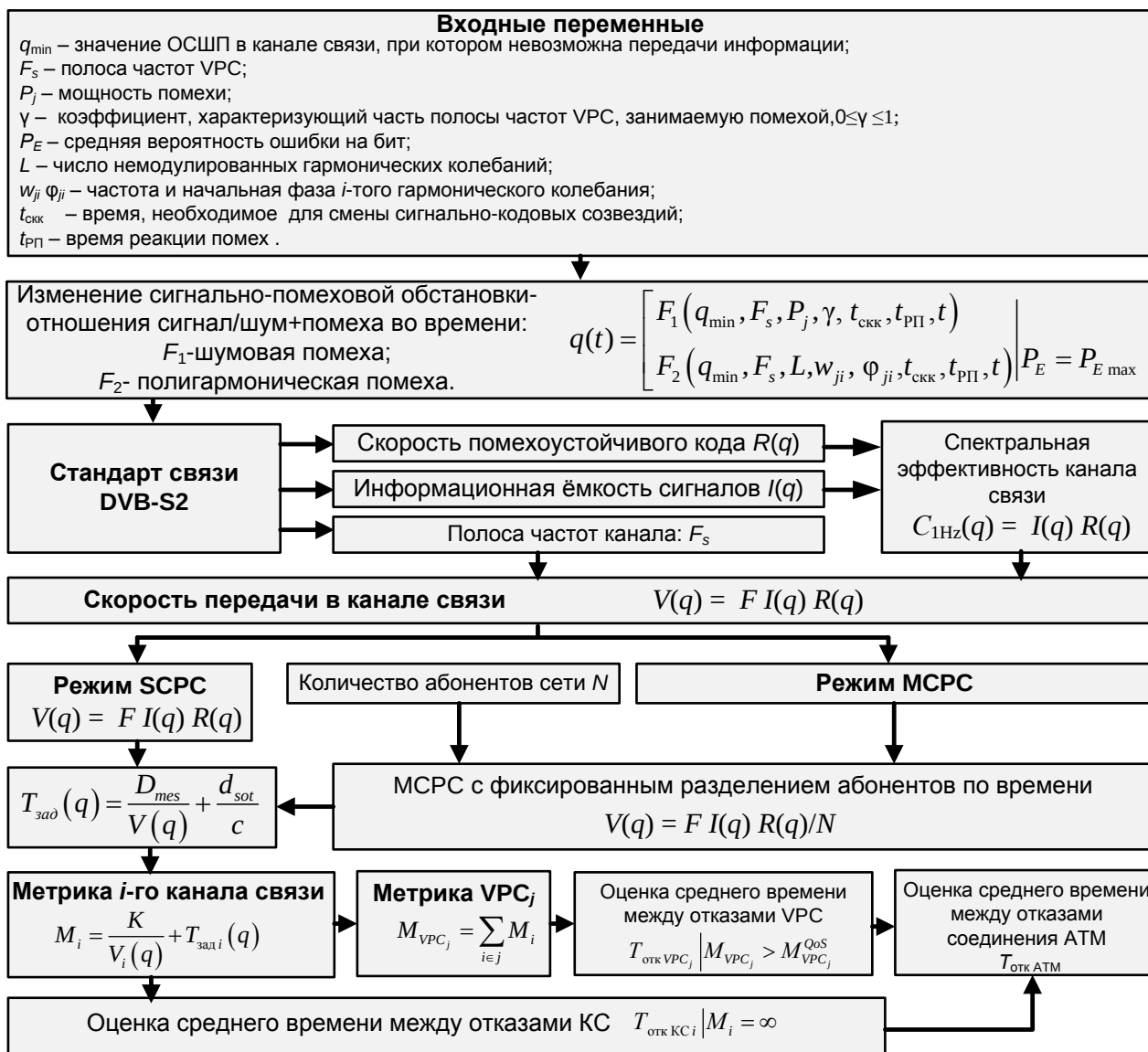


Рис. 5. Схема взаимосвязи аналитических соотношений в модели функционирования АТМ-маршрутизатора при изменении метрики каналов связи вследствие воздействия средств РЭП

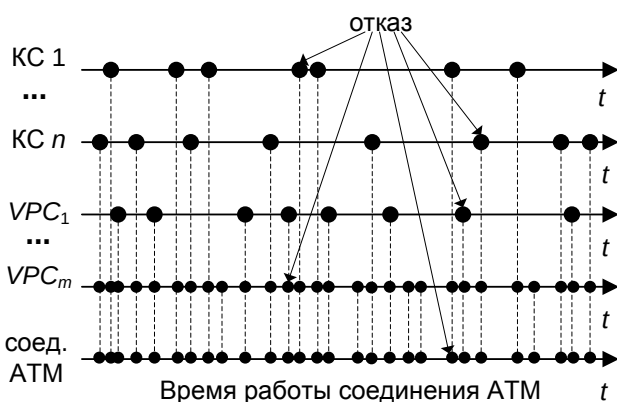


Рис. 6. Моменты отказов отдельных КС и VPC, приводящие к отказу соединения АТМ

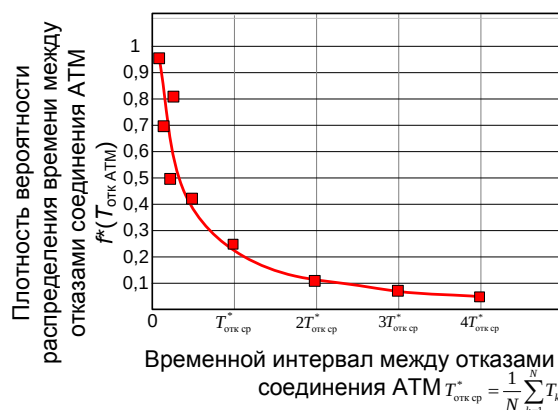


Рис. 7. Плотностью вероятности распределения времени между отказами соединения АТМ

Модель функционирования межузловое соединения ТНКСС в условиях воздействия средств РЭП

Разработанная модель формализует процесс функционирования межузловое соединения ТНКСС и необходима для установления зависимости между временными параметрами сигнализации и отказа КС, как эффекта от воздействия средств РЭП на сетевом уровне ЭМВОС [23-25]. Диагностика отказов КС в протоколе PNNI осуществляется путем обмена соседними АТМ-маршрутизаторами служебными пакетами Hello с периодичностью, определяемой для каждого КС значением времени диагностики отказа в ИНС $T_{\text{диагн}}$. В рамках разработанной модели процесс функционирования межузловое соединения ТНКСС формализован в виде марковского процесса перехода между различными состояниями (рис. 8):

S_0 – «работоспособное состояние» соединения ТНКСС, когда служебные пакеты Hello вовремя принимаются АТМ-маршрутизаторами;

S_1 – «состояние отказа», когда соединение ТНКСС отказ не диагностировало и продолжает использовать КС как работоспособный, то есть состояние, в котором КС подавлен средствами РЭП, однако установить факт этого подавления возможно лишь в случае неприбытия в расчетное время служебного пакета Hello;

S_2 – «состояние ожидания», когда соединение ТНКСС диагностировало отказ КС, но ожидает восстановления связи в нем. Это состояние, характеризующееся неприбытием в расчетное время служебного пакета Hello, однако ввиду возможности его случайной утери (сбоя в КС) осуществляется подтверждение факта подавления КС на протяжении времени ожидания восстановления связи в ИНС $T_{\text{ож}}$, в течение которого служебные пакеты Hello не поступают;

S_3 – «состояние реконфигурации», когда соединение ТНКСС диагностировало, что восстановление связи в КС не произошло, и запущен процесс реконфигурации путей в ИНС в интересах восстановления работоспособности.

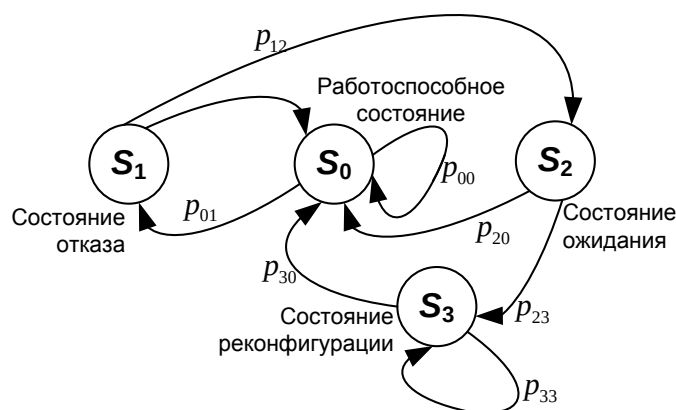


Рис. 8 Марковская модель функционирования межузловое соединения ТНКСС
в условиях воздействия средств РЭП

Вероятность p_{00} того, что интервал диагностики $T_{\text{диагн}}$ меньше времени среднего времени между отказами КС $T_{\text{отк КС}}$, то есть КС за время диагностики не отказал и продолжает работать:

$$p_{00} = P(T_{\text{диагн}} < T_{\text{отк КС}}) = e^{-\frac{T_{\text{диагн}}}{T_{\text{отк КС}}}}. \quad (10)$$

Вероятность p_{01} того, что интервал диагностики $T_{\text{диагн}}$ больше времени среднего времени между отказами КС $T_{\text{отк КС}}$, то есть канал связи за время диагностики $T_{\text{диагн}}$ отказал и во время проведения диагностики объект установил этот отказ - система перешла в «состояние отказа»:

$$p_{01} = P(T_{\text{диагн}} > T_{\text{отк КС}}) = 1 - e^{-\frac{T_{\text{диагн}}}{T_{\text{отк КС}}}}. \quad (11)$$

Вероятность p_{10} того, что за интервал диагностики $T_{\text{диагн}}$ канал успел и отказать, и восстановиться, в результате система вновь перешла в «работоспособное состояние»:

$$p_{10} = P(T_{\text{диагн}} > T_{\text{отк КС}} + T_{\text{вост КС}}) = 1 - e^{-\frac{T_{\text{диагн}}}{T_{\text{отк КС}} + T_{\text{вост КС}}}}. \quad (12)$$

Вероятность p_{12} того, что за интервал диагностики $T_{\text{диагн}}$ канал успел отказать, но не успел восстановиться и система перешла в «состояние ожидания» восстановления связи:

$$p_{12} = P(T_{\text{диагн}} < T_{\text{отк КС}} + T_{\text{вост КС}}) = e^{-\frac{T_{\text{диагн}}}{T_{\text{отк КС}} + T_{\text{вост КС}}}}. \quad (13)$$

Вероятность p_{20} того, что за время интервала диагностики $T_{\text{диагн}}$ и время ожидания $T_{\text{ож}}$ канал успел и отказать, и успел восстановиться, в результате система вернулась в «работоспособное состояние»:

$$p_{20} = P(T_{\text{диагн}} + T_{\text{ож}} > T_{\text{отк КС}} + T_{\text{вост КС}}) = 1 - e^{-\frac{T_{\text{диагн}} + T_{\text{ож}}}{T_{\text{отк КС}} + T_{\text{вост КС}}}}. \quad (14)$$

Вероятность p_{23} того, что за время интервала диагностики $T_{\text{диагн}}$ и время ожидания $T_{\text{ож}}$ канал успел отказать, но не успел восстановиться, и система перешла в «состояние реконфигурации»:

$$p_{23} = P(T_{\text{диагн}} + T_{\text{ож}} < T_{\text{отк КС}} + T_{\text{вост КС}}) = e^{-\frac{T_{\text{диагн}} + T_{\text{ож}}}{T_{\text{отк КС}} + T_{\text{вост КС}}}}. \quad (15)$$

Время реконфигурации принято распределенным по экспоненциальному закону с математическим ожиданием $T_{\text{рек}}$. В этом случае вероятность p_{33} того, что за время $T_{\text{рек}}$ объект успел изменить свои параметры и система перешла в «работоспособное состояние»:

$$p_{30} = P(t > T_{\text{рек}}) = e^{-1}, \quad (16)$$

а вероятность того, что за тоже время $T_{\text{рек}}$ продолжается реконфигурация:

$$p_{33} = P(t < T_{\text{рек}}) = 1 - e^{-1}. \quad (17)$$

Формализация функционирования соединения ТНКСС в виде марковского процесса с данными переходными вероятностями p_{ij} позволяет составить уравнения для состояний системы, при допущении о стационарности процесса ее функционирования:

$$\begin{cases} P(S_1)p_{10} + P(S_2)p_{20} + P(S_3)p_{30} - P(S_0)p_{01} - P(S_0)p_{00} + P(S_0)p_{00} = 0 \\ P(S_0)p_{01} - P(S_1)p_{12} - P(S_1)p_{10} = 0 \\ P(S_1)p_{12} - P(S_2)p_{20} - P(S_2)p_{23} = 0 \\ P(S_2)p_{23} - P(S_3)p_{30} - P(S_3)p_{33} + P(S_3)p_{33} = 0 \\ P(S_0) + P(S_1) + P(S_2) + P(S_3) = 1 \end{cases}$$

Решение данной системы уравнений позволит получить вероятности нахождения системы в соответствующих состояниях, в зависимости от переходных вероятностей:

$$\begin{cases} P(S_0) = \frac{P_{30}}{P_{01}P_{30} + P_{01}P_{12}P_{30} + P_{30} + P_{01}P_{12}P_{23}} \\ P(S_1) = \frac{P_{01}P_{30}}{P_{01}P_{30} + P_{01}P_{12}P_{30} + P_{30} + P_{01}P_{12}P_{23}} \\ P(S_2) = \frac{P_{01}P_{12}P_{30}}{P_{01}P_{30} + P_{01}P_{12}P_{30} + P_{30} + P_{01}P_{12}P_{23}} \\ P(S_3) = \frac{P_{01}P_{12}P_{23}}{P_{01}P_{30} + P_{01}P_{12}P_{30} + P_{30} + P_{01}P_{12}P_{23}} \\ P(S_0) + P(S_1) + P(S_2) + P(S_3) = 1 \end{cases} \quad (18)$$

Схема расчета вероятностей нахождения межузлового соединения ТНКСС в различных состояниях приведена на рис. 9.

Вероятность нахождения соединения ТНКСС в работоспособном состоянии $P(S_0)$ по своему физическому смыслу соответствует коэффициенту готовности ИНС K_{Γ} . Таким образом, зависимость коэффициента готовности ИНС от временных интервалов сигнализации и отказов КС вследствие воздействия средств РЭП определяется выражением:

$$K_{\Gamma} = P(S_0) = \frac{e^{-1}}{\left(1 - e^{-\frac{1}{T_{\text{отк КС}}} T_{\text{диагн}}}\right) \left(1 + e^{-\frac{1}{T_{\text{отк КС}} + T_{\text{вост КС}}} T_{\text{диагн}}} + (1 - e^{-\frac{1}{T_{\text{отк КС}}} T_{\text{диагн}}})^{-1} + e^{-\frac{1 - 2T_{\text{диагн}} + T_{\text{ож}}}{T_{\text{отк КС}} + T_{\text{вост КС}}}}\right)} \quad (19)$$

Результаты исследования зависимости $P(S_i)$ от значений $T_{\text{диагн}}$ и $T_{\text{ож}}$, нормированных к среднему времени между отказами КС $T_{\text{отк КС}}$, при различных значениях $T_{\text{вост КС}}$ с учетом следующих ограничений: $T_{\text{отк}}=1$; $T_{\text{диагн}}=1T_{\text{отк КС}} \dots 3T_{\text{отк КС}}$; $T_{\text{ож}}=1T_{\text{диагн}} \dots 5T_{\text{диагн}}$; $T_{\text{рек}}=10T_{\text{отк КС}}$; $T_{\text{вост КС}}=0,01, 0,25, 1$ приведены на рис. 10 а-в.

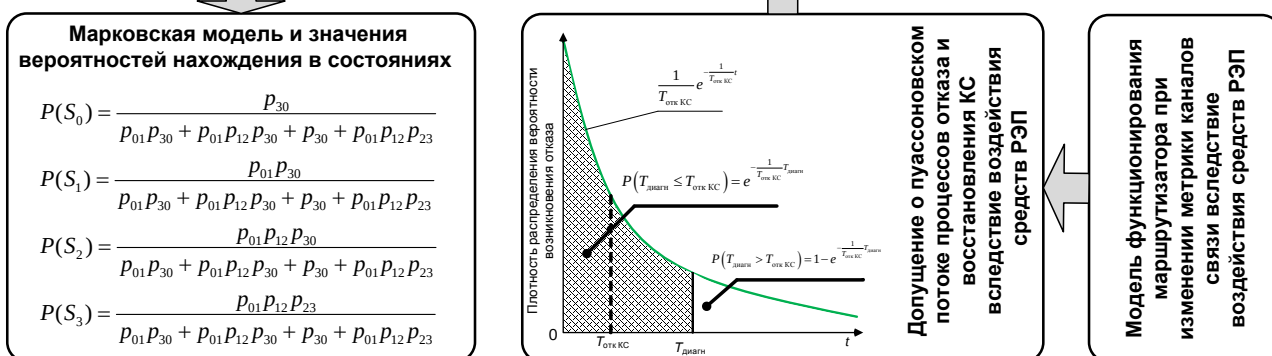
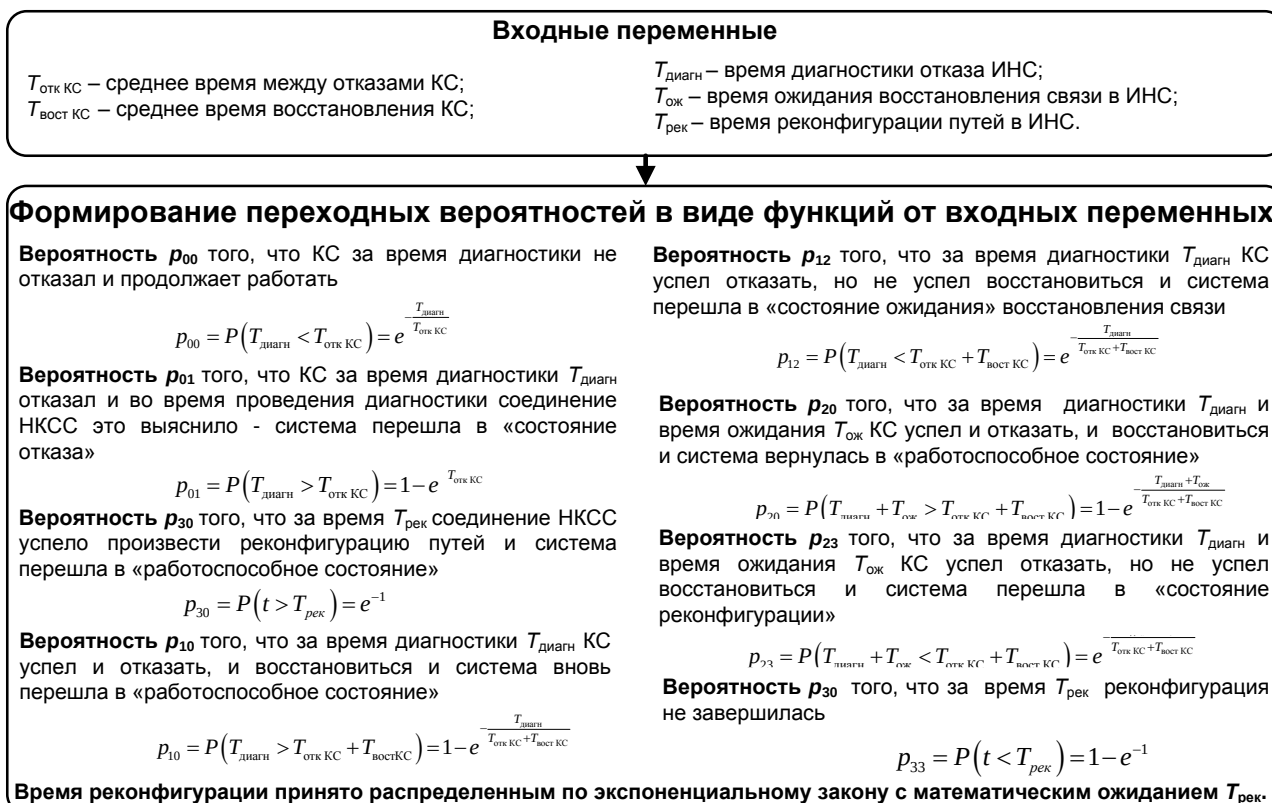


Рис. 9. Схема расчета вероятностей нахождения объекта связи в различных состояниях

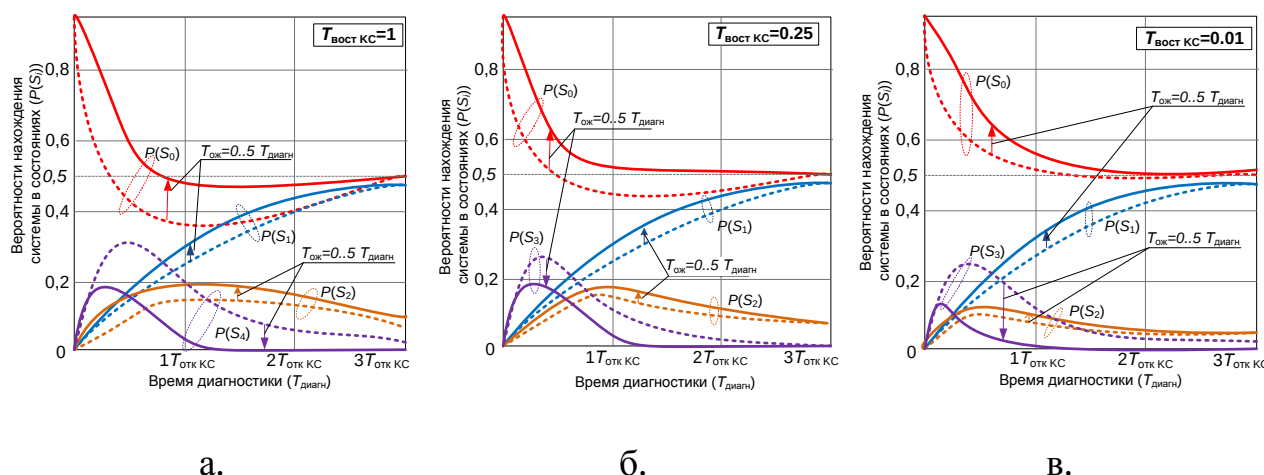


Рис. 10. Зависимости конечных вероятностей состояний системы $P(S_i)$ от $T_{\text{диагн}}$, $T_{\text{ож}}$, $T_{\text{вост КС}}$

Анализ графических зависимостей, представленных на рис. 10. а-в, позволяет сделать следующие выводы.

- 1) Отношение $T_{ож}/T_{диагн}$ влияет на быстроту схождения $P(S_i)$ к предельным значениям. При $T_{ож} = 0T_{диагн}$, значения $P(S_0)$, $P(S_1)$, $P(S_2)$ достигают своего минимального значения, а $P(S_3)$ – максимального. Увеличение этого отношения выше значения $T_{ож}/T_{диагн}=5$ не влияет на значения вероятностей нахождения системы в различных состояниях $P(S_i)$.
- 2) При увеличении значений $T_{диагн}$ вероятность работоспособного состояния $P(S_0)$ снижается и стремится к своему предельному значению $P(S_0) \rightarrow 0,5$. При этом значения K_r определяют наличие и значение минимума функции $P(S_0)$.
- 3) Уже при значениях $T_{диагн} = 0,25T_{отк\ КС}$ ($T_{ож} = 5T_{диагн}$) значение вероятности нахождения в работоспособном состоянии $P(S_0)$ принимает критическое значение $P(S_0) = 0,9$, а при меньшем значении $T_{ож} < 5T_{диагн}$ происходит снижение значений вероятности до $P(S_0) < 0,9$, что является неприемлемым значением для коэффициента готовности ИНС K_r .
- 4) При уменьшении $T_{диагн}/T_{отк\ КС}$ снижается влияние значение среднего времени восстановления КС $T_{вост\ КС}$ на вероятности $P(S_i)$, а при $T_{диагн} \leq 0,01T_{отк\ КС}$ вероятность нахождения системы в работоспособном состоянии $P(S_0)$ практически от $T_{вост\ КС}$ не зависит.

Алгоритм маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС

Целью разработки алгоритма является сокращение времени реконфигурации $T_{рек}$. В работе [26] показано, что для резервируемых КС время реконфигурации $T_{рек}$ определяется в соответствии с выражением (20):

$$T_{рек} = T_{увед} + T_{ПНП} + T_{перекл}, \quad (20)$$

где $T_{увед}$ – время уведомления об отказе КС узла, ответственного за реконфигурацию путей, $T_{ПНП}$ – время, необходимое для нового поиска кратчайших путей, $T_{перекл}$ – время переключения на резервные пути.

Время уведомления об отказе КС узла, ответственного за реконфигурацию путей, $T_{увед}$ зависит от времени передачи между отдельными узлами сообщения об отказе T_p и от количества участков сети d_{ij} , между узлом, обнаружившим отказ КС (узел i), и узлом, ответственным за переключение путей (узел j) [26].

$$T_{увед\ i} = T_p d_{ij}, \quad (21)$$

Время, необходимое для нового поиска кратчайших путей, $T_{ПНП}$ зависит от используемого алгоритма поиска кратчайших путей, а также размера СС.

Время переключения на резервные пути $T_{перекл}$ зависит от быстродействия маршрутизатора (коммутатора).

Таким образом, сокращение времени реконфигурации $T_{рек}$ возможно осуществить путем снижения времени уведомления об отказе КС узла,

ответственного за реконфигурацию путей, $T_{увед}$ и времени, необходимого для нового поиска кратчайших путей, $T_{ппп}$. Снижение времени уведомления об отказе КС узла, ответственного за реконфигурацию путей, $T_{увед}$ достигается путем организации возможности переключения на резервные маршруты в случае отказа КС узлом, ближайшим к этому отказу. В этом случае, согласно выражению (21), количество участков сети d_{ij} , между узлом, обнаружившим отказ КС, и узлом, ответственным за переключение путей, а, следовательно, и сам временной показатель $T_{увед}$ будут равно нулю. Снижение времени, необходимого для нового поиска кратчайших путей, $T_{ппп}$, достигается посредством заблаговременного поиска как кратчайших, так и резервных путей в СС и занесение их в таблицы маршрутизации.

В ходе разработки алгоритма проведена модификации алгоритма Дейкстры, и в него дополнительно внесены изменения, направленные на расширение его функциональности, связанной с формированием резервных путей в соответствии с вышеуказанными положениями [27-28]. В основу предлагаемой модификации алгоритма Дейкстры являются следующие положения.

- 1) При достижении очередной вершины, запоминаются исходящие вершины входящих в эту вершину ребер, как потенциальные элементы будущего резервного пути к этой вершине (рис. 11).
- 2) При очередном шаге функционирования, алгоритма, достигнутая очередная вершина проверяется как потенциальный элемент резервного пути для всех уже достигнутых вершин. Если она является потенциальным элементом резервного пути, формируется резервный путь к ранее достигнутой вершине, через только что достигнутую (рис. 12).

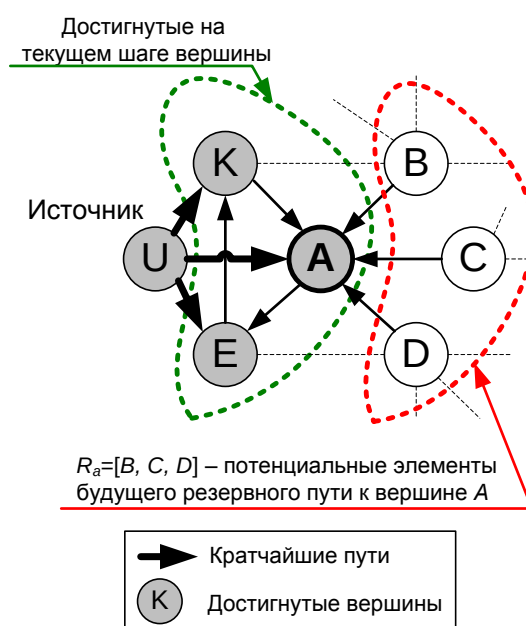
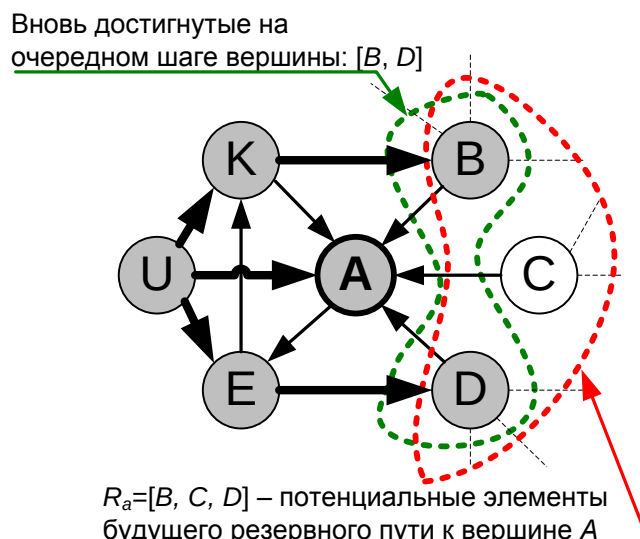


Рис. 11. Запись потенциальных элементов будущего резервного пути к вершине



Сравнение $[B, C, D]$ и $[B, D]$ приводит к выводу, что резервные пути к A лежат через B и D.

Рис. 12. Формирование резервного пути к вершине

- 3) Если к ранее достигнутой вершине уже были сформированы резервные пути и она участвует в создании нового резервного пути к очередной вершине, то к очередной вершине формируется множество резервных путей с включением в них всех возможных вариантов резервных путей сформированных ранее. Причем, если в резервный путь входит сама очередная вершина то такой путь, во избежание циклов, в резервные не включается (рис. 13).
- 4) Все резервные пути к вершинам сети упорядочиваются в соответствии с минимизацией весов и вносятся в таблицу маршрутизации наряду с кратчайшим путем. При отказе элементов кратчайшего пути для передачи выбирается резервный путь с минимальным суммарным весом, не содержащий отказавшие элементы (рис. 14).

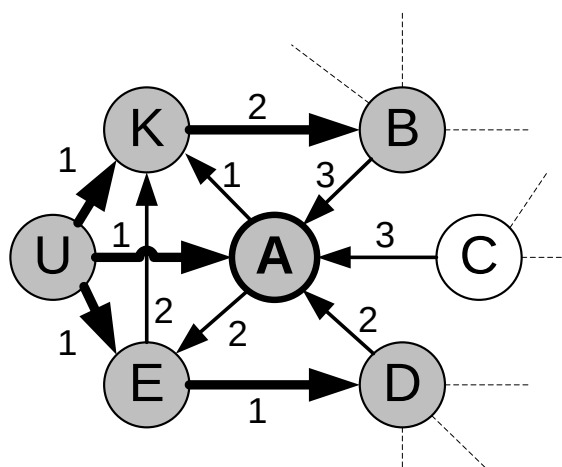


Рис. 13. Пример построения резервных путей к вершине

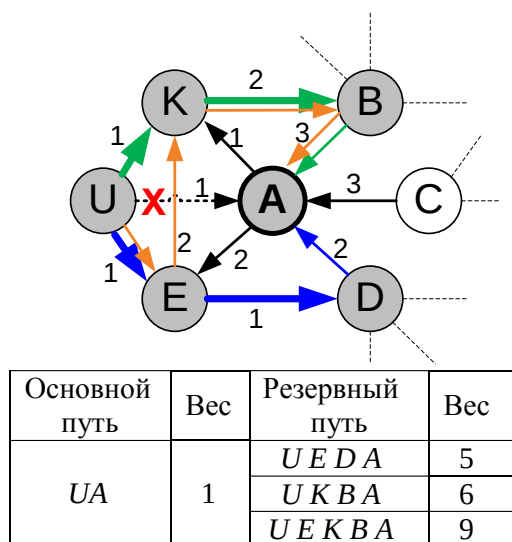


Рис. 14. Пример построения резервных путей к вершине

Схема алгоритма маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС приведена на рис. 15.

Входными параметрами алгоритма являются: ориентированный граф сети $G(U, V)$; количество вершин в графе n ; веса ребер, соединяющих произвольные i -ую и j -ую вершины $V(U_i, U_j)$.

Для обеспечения работы алгоритма помимо имеющихся множеств (P – множество помеченных вершин, L – множество смежных помеченных вершин, множество расстояний до помеченных и вершин от начальной вершины) вводятся следующие дополнительные множества.

- 1) R – множество вершин потенциальных резервных путей. В это множество вносятся достигнутые вершины, смежные рассматриваемой. В дальнейшем, элементы множества используются при нахождении резервных путей.
- 2) S – множество весов ребер потенциальных резервных путей. В это множество вносятся веса ребер, исходящих из вершин, вносимых в множество R и входящих в рассматриваемую вершину.
- 3) Z – множество резервных путей в вершину, содержит резервные пути в рассматриваемую вершину, сформированные в результате проведения логических операций над входящими в него элементами и элементами множества R и L .
- 4) S – множество весов резервных путей к вершине. Это множество содержит веса путей из множества Z и используется для ранжировки резервных путей при выводе результатов работы алгоритма.

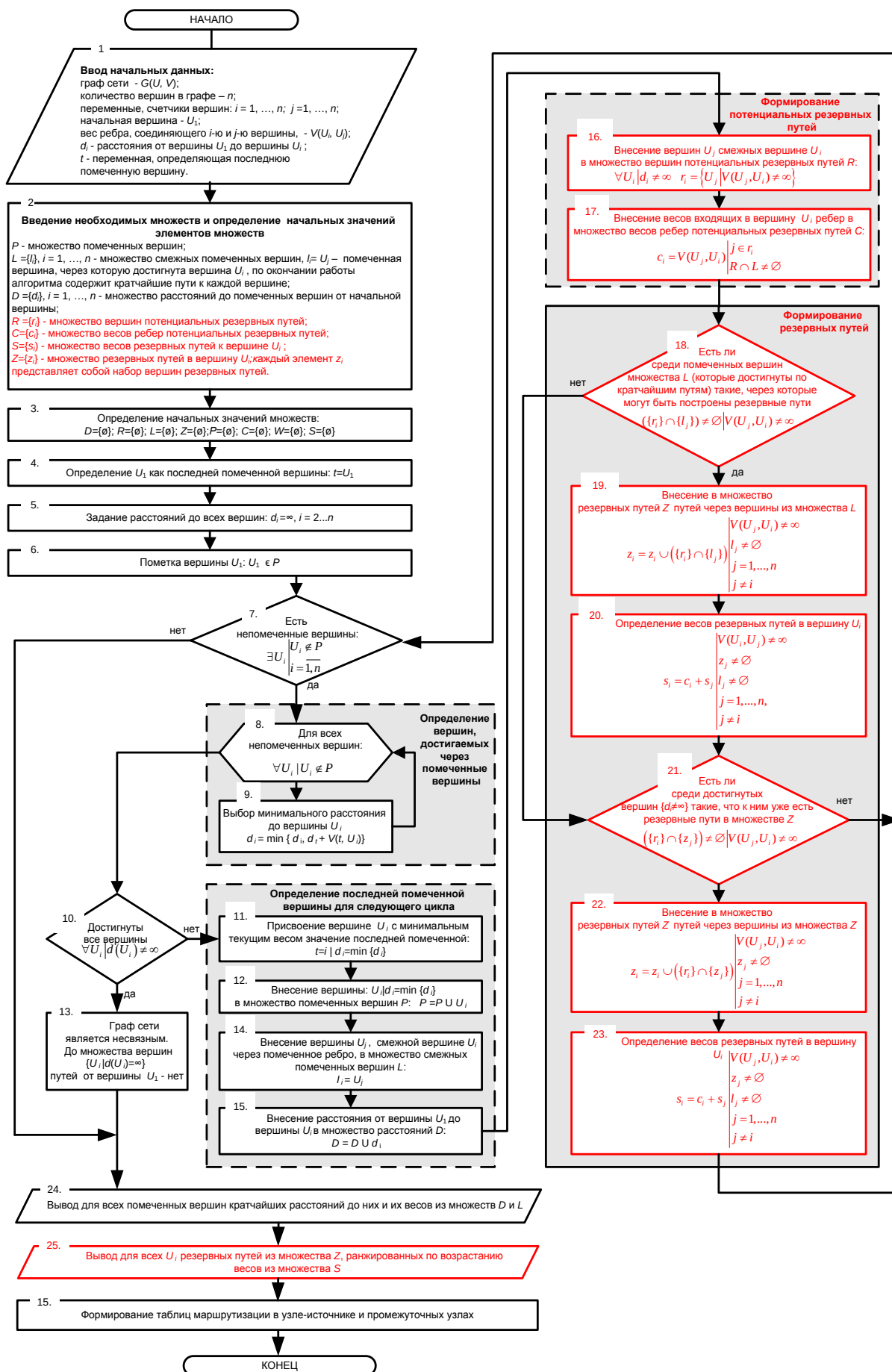


Рис. 15. Алгоритм маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС

К новым элементам алгоритма относятся блоки 16-23, 25. В блоках 16-17 реализуется формирование элементов множества вершин R к текущей рассматриваемой вершине за счет использования положения № 1 по модификации алгоритма. Далее, в блоках 18-23, путем пересечения элементов множества R и L , а также Z , осуществляется формирование элементов множества Z с учетом положения № 2 по модификации алгоритма. В блоке 25 осуществляется ранжировка резервных путей по сумме весов, входящих в их состав ребер.

Алгоритм адаптивного изменения временных параметров сигнализации в межузловом соединении ТНКСС в условиях воздействия средств РЭП

С учетом выражения (9) для коэффициента готовности ИНС K_T и уменьшая время реконфигурации путей в ИНС $T_{рек}$ благодаря использованию алгоритма маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС, возможно определить значения временных параметров сигнализации, обеспечивающих заданный уровень вероятности своевременной доставки пакета $P_{сд}$ согласно выражению (8). Для этого был разработан алгоритм адаптивного изменения временных параметров сигнализации в межузловом соединении ТНКСС в условиях воздействия средств РЭП, представленный на рис. 16.

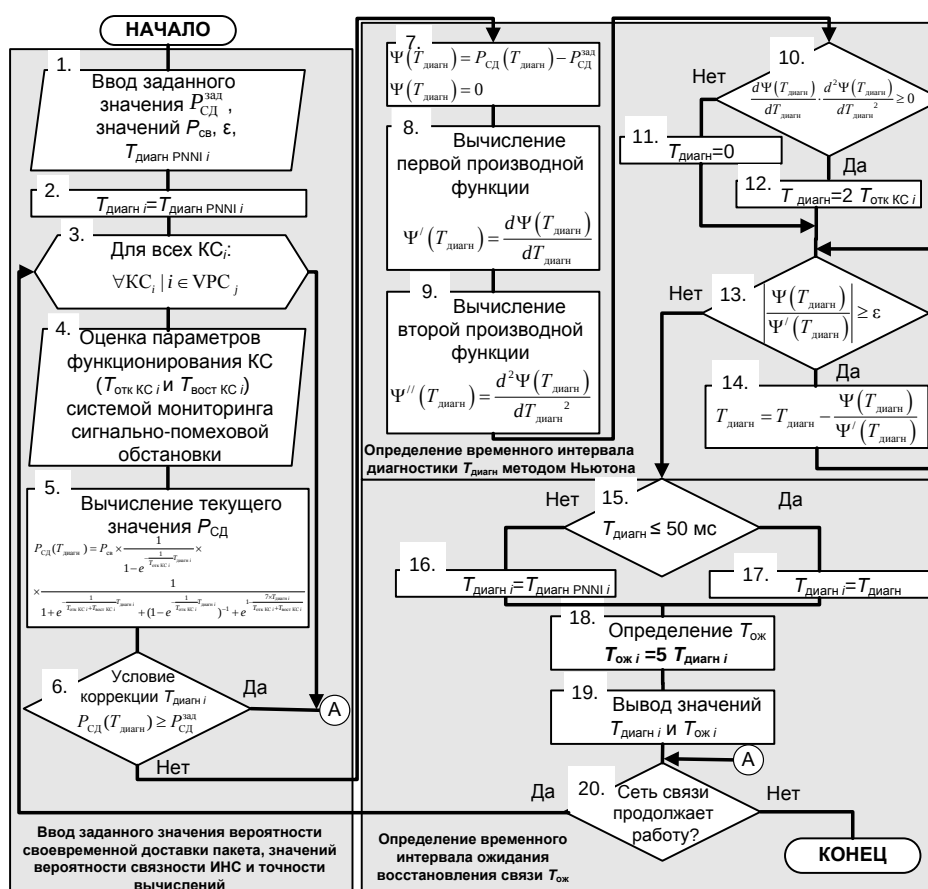


Рис. 16. Алгоритм адаптивного изменения временных параметров сигнализации в межузловом соединении ТНКСС в условиях воздействия средств РЭП

Входными параметрами алгоритма являются: заданный уровень вероятности своевременной доставки пакета $P_{\text{СД}}^{\text{зад}}$; среднее время между отказами КС $T_{\text{отк КС}}$; значение вероятности связности ИНС $P_{\text{св}}$; среднее время восстановления КС $T_{\text{вост КС}}$; заданная точность вычислений ε .

Значение вероятности связности ИНС $P_{\text{св}}$ заблаговременно определяется исходя из структуры ТНКСС и вероятностей работоспособного состояния отдельных ее элементов (КС и узлов связи). Определение значения среднего времени между отказами КС $T_{\text{отк КС}}$ осуществляется системой мониторинга сигнально-помеховой обстановки. Среднее время восстановления КС $T_{\text{вост КС}}$ определяется временными затратами, связанными со сменой сигнально-кодовых созвездий с целью восстановления работоспособности КС при превышении ОСШП значений, заданных в технологии DVB-S2. В алгоритме используются обоснованные в рамках модели функционирования межузловое соединения ТНКСС в условиях воздействия средств РЭП отношение $T_{\text{ож}}/T_{\text{диагн}}=5$ и значение среднего времени восстановления КС $T_{\text{вост КС}}=0$. Ключевыми блоками алгоритма являются блоки 7-14, в которых осуществляется численный расчет времени диагностики $T_{\text{диагн}}$ методом Ньютона. Более подробно алгоритм описан в работе [29].

Оценка повышения устойчивости ТНКСС СВС ВС РФ при использовании разработанных алгоритмов

Проведенное в работе моделирование в среде MathCad показало, что использование алгоритма маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС СВС ВС РФ позволяет повысить отношение $T_{\text{диагн}}/T_{\text{отк КС}}$ при котором обеспечивается заданный уровень вероятности своевременной доставки пакета $P_{\text{СД}}^{\text{зад}}$, на 60-65%, в зависимости от значения вероятности связности ИНС $P_{\text{св}}$ (рис. 17.), вследствие этого прирост вероятности своевременной доставки пакета $P_{\text{СД}}$ может достигать 7%, в зависимости от имеющегося отношения $T_{\text{ож}}/T_{\text{диагн}}$ и значения $P_{\text{св}}$ (рис. 18.). Изменение целевых показателей работы (8) в зависимости от значения среднего времени между отказами КС $T_{\text{отк КС}}$ приведено на рис. 19. а-б. Уменьшение значения вероятности связности ИНС $P_{\text{св}}$ в случае, если не используются разработанные алгоритмы приводит к снижению вероятности своевременной доставки пакета $P_{\text{СД}}$, а в случае, если используются разработанные алгоритмы – к повышению минимального значения времени диагностики $T_{\text{диагн}}$, при котором обеспечивается заданное значение вероятности своевременной доставки пакета $P_{\text{СД}}^{\text{зад}}$. Использование разработанных алгоритмов позволяет обеспечить заданное значение вероятности своевременной доставки пакета $P_{\text{СД}}^{\text{зад}} = 0,9 | T_{\text{дост}}^{\text{зад}} = 3 \text{ с.}$ при значениях $T_{\text{отк КС}} > 1,2 \text{ с.}$ при этом эффективность их использования E_y (рис. 20.) при $T_{\text{отк КС}} = 1,2 \dots 600 \text{ с}$ достигает 80%, что позволяет говорить о достижении цели диссертационного исследования.

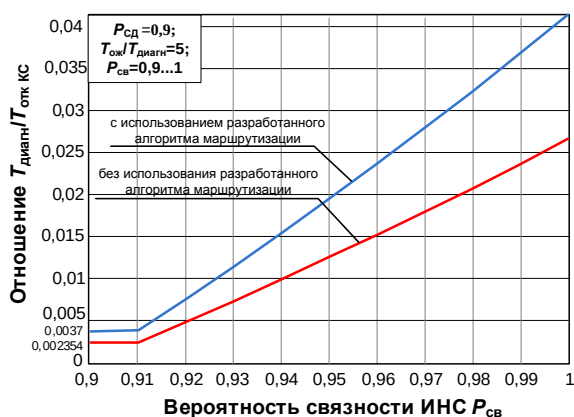


Рис. 17. Зависимость требуемого отношения $T_{\text{диагн}}/T_{\text{отк КС}}$ для обеспечения $P_{\text{сд}}^{\text{зад}}$ при различных значениях $P_{\text{св}}$

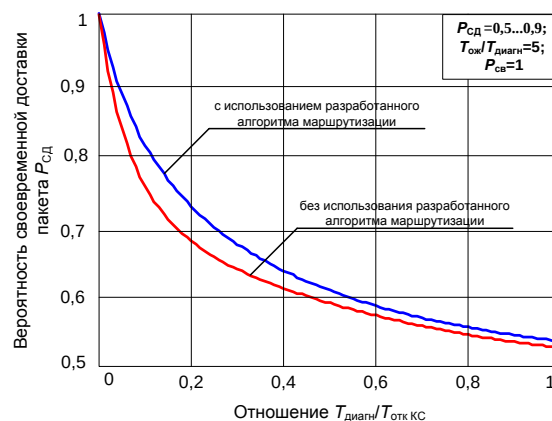
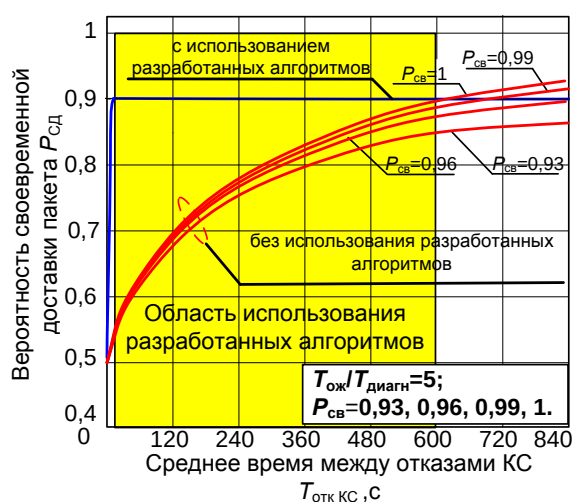
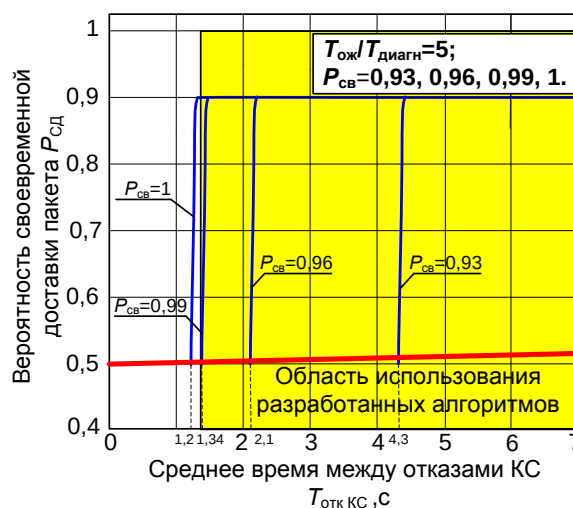


Рис. 18. Зависимость $P_{\text{сд}}$ от отношения $T_{\text{диагн}}/T_{\text{отк КС}}$



а.



б.

Рис. 19. Зависимость $P_{\text{сд}}$ от $T_{\text{отк КС}}$

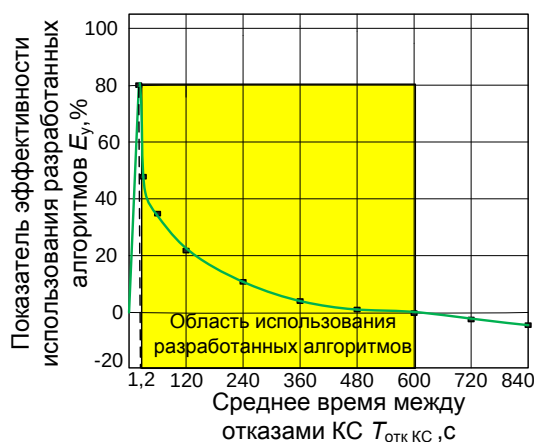


Рис. 20. Зависимость E_y от $T_{\text{отк КС}}$

Разработаны предложения по технической реализации разработанных алгоритмов для математического обеспечения коммутатора пакетов путем дополнения его блоком адаптивного изменения временных параметров сигнализации и дополнительным объемом памяти для хранения информации о резервных маршрутах. Проведен военно-экономический анализ целесообразности внедрения разработанного математического обеспечения.

Выводы

В работе описаны элементы научно-методического аппарата маршрутизации информационных потоков, применение которых позволяет повысить устойчивости ТНКСС СВС ВС РФ в условиях воздействия средств РЭП.

Научная новизна полученных результатов заключается в следующем:

- 1) Впервые полученные модель функционирования АТМ-маршрутизатора и модель межузловое соединения ТНКСС в условиях воздействия средств РЭП, отличающиеся от известных возможностью оценки параметров КС сетевого уровня ЭМВОС как результата преднамеренных воздействий средств РЭП, с учетом схем адаптивного выбора вида модуляции сигналов и скорости помехоустойчивого кодирования, а также оригинальным переходом от соотношения временных интервалов сигнализации к вероятностным параметрам марковской модели, позволяющим получить аналитические выражения для зависимости вероятности нахождения межузловое соединения ТНКСС в работоспособном состоянии от значений временных интервалов сигнализации.
- 2) Алгоритм маршрутизации информационных потоков по кратчайшим и резервным путям на основе использования структурной избыточности ТНКСС, отличающийся от используемого в протоколе PNNI алгоритма Дейкстры новыми функциональными элементами, обеспечивающими возможность поиска в структуре ТНКСС резервных путей одновременно с ведением поиска кратчайших путей, что позволяет снизить время реконфигурации путей в ТНКСС, вызванное подавлением КС ТНКСС средствами РЭП.
- 3) Алгоритм адаптивного изменения временных параметров сигнализации в межузловое соединении ТНКСС в условиях воздействия средств РЭП, основанный на использовании оригинальной модели функционирования межузловое соединения ТНКСС в условиях воздействия средств РЭП для обоснования временных параметров сигнализации при заданных условиях воздействия средств РЭП. Применение данного алгоритма обеспечивает более адекватную диагностику факта подавления КС на сетевом уровне ЭМВОС, что позволяет повысить устойчивость ТНКСС путем динамического изменения временных интервалов сигнализации исходя из оценки интенсивности воздействия средств РЭП.

Литература

1. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.
2. Надежность и живучесть систем связи / Под ред. Дудника Б. Я. М.: Радио и связь, 1984. 350 с.
3. Нетес В.А. Надежность сетей связи в период перехода к NGN // Вестник связи. 2007. № 9. С. 1-8.
4. Киселев Л. К., Маркелов А. П., Воробьев Б. В. Концептуальные основы обеспечения устойчивости сетей связи // Электросвязь. 1994. № 2.
5. Юрасова Л. В., Кондратов С. Ф. Проблемы разработки нормативных правовых актов по вопросам применения средств связи // Электросвязь. 2007. № 3.
6. ГОСТ 5311 – 2008. Устойчивость функционирования сети связи общего пользования. М.: Стандартинформ, 2008. 15 с.
7. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. №4. С. 69-79.
8. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 183 с.
9. Назаров А. Н., Сычев К. И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. Красноярск: Поликом, 2010. 389 с.
10. Ададулов С. Е., Чатоян С. К., Зелинский А. Е. Показатели устойчивости информационного обмена в защищенных телекоммуникационных системах // Проблемы информационной безопасности. Компьютерные системы. 1999. № 2. С. 100-107.
11. Ушаков И. А. Курс теории надежности систем: учебное пособие для ВУЗов. М.: Дрофа, 2008. 239 с.
12. Макаренко С. И. Анализ воздействия преднамеренных помех на функционирование расширенного протокола маршрутизации внутреннего шлюза (EIGRP) // Информационные технологии моделирования и управления. 2010. № 2 (61). С. 223-229.
13. Фокин В. Г. Оптические системы передачи и транспортные сети. Учебное пособие. М.: Эко-Трендз, 2008. 271 с.
14. ETSI EN 302 307. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation system for Broadcasting Interactive Services, News Gathering and other broadband satellite applications.
15. ETSI EN 300 421. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz satellite services.

16. ETSI EN 301 210. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for Digital Satellite News Gathering (DSNG) and other contribution applications by satellite.
17. ETSI TR 102 376 v. 1.1.1 (2005-02). Digital Video Broadcasting (DVB); User guidelines for the second generation system for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2).
18. ETSI EN 300 744. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television.
19. Стандарт DVB-S2. Система цифрового ТВ вещания. // Контур–М [Электронный ресурс]. – Режим доступа: URL: www.konturm.ru/tech.php?id=dvbs2
20. Макаренко С. И. Модели воздействия средств радиоэлектронной борьбы на систему связи на основе методов популяционной динамики // Вестник Воронежского государственного технического университета. 2011. Т. 7. № 1. С. 96-99.
21. Макаренко С. И. Оценка качества обслуживания пакетной радиосети в нестационарном режиме в условиях воздействия внешних дестабилизирующих факторов // Журнал радиоэлектроники. 2012. № 6. URL: jre.cplire.ru/jre/jun12/9/text.pdf (дата обращения 11.08.2015).
22. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально-помеховой обстановки // Журнал радиоэлектроники. 2014. № 10. URL: <http://jre.cplire.ru/jre/oct14/3/text.pdf> (дата обращения 11.08.2015).
23. Макаренко С. И., Михайлов Р. Л., Рюмшин К. Ю. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147.
24. Макаренко С. И., Михайлов Р. Л., Модель функционирования коммутатора в сети с использованием протокола покрывающего дерева STP и исследование устойчивости сети в условиях ограниченной надежности каналов связи // Радиотехнические и телекоммуникационные системы. 2013. № 2. С. 61-68.
25. Макаренко С. И., Михайлов Р. Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. 2014. Том 12. № 2. С 44-49.
26. Егунов М. М., Шувалов В. П. Анализ структурной надежности транспортной сети // Вестник СибГУТИ. 2012. № 1. С. 54-60.
27. Цветков К. Ю., Макаренко С. И., Михайлов Р. Л. Формирование резервных путей на основе алгоритма Дейкстры с целью повышения устойчивости информационно-телекоммуникационных сетей // Информационно-управляющие системы. 2014. № 2. С. 71-78.

28. Макаренко С. И., Михайлов Р. Л. Предложения по модификации алгоритма Дейкстры для повышения устойчивости протоколов маршрутизации с использованием топологической избыточности сетей единой спутниковой системы связи 3-го поколения // Сборник алгоритмов и прикладных задач. СПб.: ВКА имени А.Ф.Можайского. 2013. № 30. С. 135-143.

29. Макаренко С. И., Михайлов Р. Л. Адаптация параметров сигнализации в протоколе маршрутизации с установлением соединений при воздействии на сеть дестабилизирующих факторов // Системы управления, связи и безопасности. 2015. № 1. С. 98-126. URL: <http://journals.intelgr.com/sccs/arhov/2015-01/07-Makarenko.pdf> (дата обращения 11.08.2015).

References

1. Antonovich P. I., Makarenko S. I., Mikhailov R. L., Ushanev K. V. Perspektivnye sposoby destruktivnogo vozddeistviia na sistemy voennogo upravleniia v edinom informatsionnom prostranstve [Perspective Ways of Influence on Military Centric Control System]. *Vestnik Akademii voennykh nauk*, 2014, vol. 48, no. 3, pp. 93-101. (In Russian).

2. Dudnik B. Ia. *Nadezhnost' i zhivuchest' sistem sviazi* [The Reliability and the Liveness of Communication Systems]. Moscow, Radio i sviaz' Publ., 1984, 350 p. (in Russian).

3. Netes V. A. Nadezhnost' setei sviazi v period perekhoda k NGN [The Reliability of Communication Networks during the Conversion for New Generation Nets (NGN)]. *Vestnik sviazi*, 2007, no. 9, pp. 1-8 (in Russian).

4. Kiselev L. K., Markelov A. P., Vorob'ev B. V. Kontseptual'nye osnovy obespecheniia ustoichivosti setei sviazi [Conceptual Frameworks of Communication Network` Sustainability]. *Telecommunication and Radio Engineering*, 1994, no. 2 (in Russian).

5. Iurasova L. V., Kondratov S. F. Problemy razrabotki normativnykh pravovykh aktov po voprosam primeneniia sredstv sviazi [The Problem Aspects of the Normative Documents of Communication Facilities` Application Developing]. *Telecommunication and Radio Engineering*, 2007, no. 3 (in Russian).

6. *State Standard 5311–2008. Stability of functioning of the public communications network*. Moscow, StandartInform, 15 p. (in Russia).

7. Mikhailov R. L., Makarenko S. I. Ocenka ustojchivosti seti svyazi v uslovijah vozdeystviia na nee destabilizirujushhih faktorov [Estimating Communication Network Stability Under the Conditions of Affecting Destabilization Factors on It]. *Radioengineering and Telecommunication Systems*, 2013, no. 4, pp. 69-79 (in Russian).

8. Bogovik A. V., Ignatov V. V. *Effektivnost' sistem voennoi sviazi i metody ee otsenki* [The Effectiveness of Military Communication System and Methods of its Rating]. Saint Petersburg, Military Academy of Communications, 2006. 183 p. (in Russian).

9. Nazarov A. N., Sychev K. I. *Modeli i metody rascheta pokazatelej kachestva funkcionirovaniya uzlovogo oborudovaniya i strukturno-setevykh parametrov setej svyazi sledujushhego pokoleniya* [The Models and the Methods of Measuring of Quality Indicators of Nodal Equipment Functioning and Network Structural Parameters of Next Generation Networks]. Krosnoyarsk, Polykom Publ., 2010. 389 p. (in Russian).
10. Adadurov S. E., Chatoian S. K., Zelinskii A. E. Pokazateli ustoichivosti informatsionnogo obmena v zashchishchennykh telekommunikatsionnykh sistemakh [The Indexes of Communication` Sustainability of Guarded Telecommunication Systems]. *Problemy informatsionnoi bezopasnosti. Komp'uternye sistemy*. 1999, no. 2, pp. 100-107 (in Russian).
11. Ushakov I. A. *Kurs teorii nadezhnosti system* [The Theory of Reliability]. Moscow, Drofa Publ., 2008. 239 p. (In Russian).
12. Makarenko S. I. Analiz vozdetsviia prednamerennykh pomekh na funktsionirovanie rasshirennogo protokola marshrutizatsii vnutrennego shliuza (EIGRP) [The Analysis of Purposeful Noise on Functioning of Enhanced Interior Gateway Protocol]. *Informatsionnye tekhnologii modelirovaniia i upravleniia*, 2010, vol. 61, no. 2, pp. 223-229 (in Russia).
13. Fokin V. G. *Opticheskie sistemy peredachi i transportnye seti* [Optical Systems of Communication and Transport Networks], Moscow, Jeko-Trendz Publ., 2008, 271 p. (in Russian).
14. ETSI EN 302 307. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation system for Broadcasting Interactive Services, News Gathering and other broadband satellite applications.
15. ETSI EN 300 421. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz satellite services.
16. ETSI EN 301 210. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for Digital Satellite News Gathering (DSNG) and other contribution applications by satellite.
17. ETSI TR 102 376 v. 1.1.1 (2005-02). Digital Video Broadcasting (DVB); User guidelines for the second generation system for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2).
18. ETSI EN 300 744. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television.
19. Standart DVB-S2. The system of digital television. *Kontur-M*, Available at: www.konturm.ru/tech.php?id=dvbs2 (accessed 11 August 2015) (in Russian).
20. Makarenko S. I. Modeli vozdetsviia sredstv radioelektronnoi bor'by na sistemu svyazi na osnove metodov populiatsionnoi dinamiki [The Models of Radio Electronic Warfare` Effect on Communication Systems Based on Methods of Population` Dynamics]. *Vestnik Voronezhskogo gosudarstvennogo tehnikeskogo universiteta*, 2011, vol. 7, no. 1, pp. 96-99 (in Russian).
21. Makarenko S. I. *Otsenka kachestva obsluzhivaniia paketnoi radioseti v nestatsionarnom rezhime v usloviakh vozdetsviia vneshnikh destabiliziruiushchikh faktorov* [The Estimation of Quality of Service of Packet Network in External

Destabilizing Factors Environment]. *Zhurnal radioelektroniki*, 2012, no. 6. Available at: jre.cplire.ru/jre/jun12/9/text.pdf (accessed 11 August 2015) (in Russian)

22. Makarenko S. I., Mikhailov R. L., Novikov E. A. Issledovanie kanal'nykh i setevykh parametrov kanala svyazi v usloviakh dinamicheski izmeniaiushcheisia signal'no–pomekhovoi obstanovki [The Research of Data Link Layer and Network Layer Parameters of Communication Channel in the Conditions Dynamic Vary of the Signal and Noise Situation]. *Journal of Radio Electronics*, 2014, no. 10. Available at: <http://jre.cplire.ru/jre/oct14/3/text.pdf> (accessed 11 August 2015) (in Russian).

23. Makarenko S. I., Ryimshin K. Yu., Mixajlov R. L. Model' funktsionirovaniia ob'ekta seti svyazi v usloviakh ogranichennoi nadezhnosti kanalov svyazi [Model of Functioning of Telecommunication Object in the Limited Reliability of Communication Channel Conditions]. *Information Systems and Technologies*, 2014, no. 6, pp. 139-147 (in Russia).

24. Makarenko S. I., Mikhailov R. L. Model' funktsionirovaniia kommutatora v seti s ispol'zovaniem protokola pokryvaiushchego dereva STP i issledovanie ustoichivosti seti v usloviakh ogranichennoi nadezhnosti kanalov svyazi [The Model of the Switch, Functioning in the Network Which Applies the Spanning Tree Protocol and the Net Stability in the Conditions of the Communication Channels Limited]. *Radiotekhnicheskie i telekommunikatsionnye sistemy*, 2013, no. 2, pp. 61-68 (in Russian).

25. Makarenko S. I., Mikhaylov R. L. Model' funktsionirovaniia marshrutizatora v seti v usloviakh ogranichennoi nadezhnosti kanalov svyazi [The Model of Functioning of the Router in the Case of Limited Reliability of Communication Canals]. *Infokommunikacionie tehnologii*, no. 2, 2014, pp. 44-49 (in Russian).

26. Egunov M. M., Shuvalov V. P. Analiz strukturnoi nadezhnosti transportnoi seti [The Analysis of Structural Reliability of Traffic Nets]. *Vestnik SibGUTY*, 2012, no. 1, pp. 54–60 (in Russian).

27. Tsvetov K. U., Makarenko S. I., Mikhailov R. L. Forming of Reserve Paths Based on Dijkstra's Algorithm in the Aim of the Enhancement of the Stability of Telecommunication Networks. *Informatsionno-upravliaiushchie sistemy*, 2014, vol. 69, no. 2, pp. 71-78 (in Russian).

28. Makarenko S. I., Mikhailov R. L. Predlozheniia po modifikatsii algoritma Deikstry dlia povysheniia ustoichivosti protokolov marshrutizatsii s ispol'zovaniem topologicheskoi izbytochnosti setei edinoi sputnikovoi sistemy svyazi 3-go pokoleniia [The Proposition of Dijkstra's Algorithm Medication for Enhancement of Routing Protocols` Sustainability with the Application of United Satellite Communication Networks` Topological Redundancy]. *Sbornik algoritmov i prikladnykh zadach*, Saint Petersburg, A. F. Mozhaisky Military Space Academy, 2013, no. 30. pp. 135-143 (in Russian).

29. Makarenko S. I., Mikhailov R. L. Signaling with Adaptation Parameters in Routing Protocol with a Connection on Influence of Destabilizing Factors. *Systems of Control, Communication and Security*, 2015, no. 1, pp. 98-126. Available at: <http://journals.intelgr.com/scs/arhov/2015-01/07-Makarenko.pdf> (accessed 11 August 2015) (in Russian).

Статья поступила 8 августа 2015 г.

Информация об авторе

Михайлов Роман Леонидович – соискатель ученой степени кандидата технических наук. Адъюнкт кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: устойчивость сетей связи, маршрутизация информационных потоков, комплексное воздействие на сети связи средств наблюдения и подавления. Тел.: +7 911 777 69 73. E-mail: mikhailov-rom2012@yandex.ru

Адрес: 197198, г. Санкт-Петербург, ул. Ждановская, д. 13.

Routing models and algorithms of transport terrestrial-cosmic military network

Mikhailov R. L.

Problem statement: Application of modern technologies of packet transmission in transport terrestrial-cosmic military network updates the issues of sustainability of their operation, which vital influence the timeliness of personnel and weapon` control system. It is shown, that known routing protocols are not able to support the requisite level of sustainability of communication in purposeful destabilizing factors `effect environment, and, therefore, the necessity of their enhancement is needed. **The aim** of this research is to increase the sustainability of communication networks by researching the routing models and algorithms of data flow in purposeful destabilizing factors `effect environment. **The method used:** The methods of probability theory, theory of reliability, theory of Markov random process and graph theory were used. **Novelty** of this issue is the introduction of the sustainability of communication` coefficient, which discounts correlation between the effect of destabilizing factors `effect environment in the fault of communication channel and the characteristic of net level of Open Systems Interconnection, also the criterion of signaling timers` decision for the enhancement of that coefficient was presented. **Result:** the model-based analysis displayed, that the application of developed algorithms allows to support the requisite level of sustainability of transport terrestrial-cosmic military network with the effectiveness amount to 80% regarding of extracted coefficient. **The practical significance** of the work encloses the evolution of developed models and algorithm up to program modification of PNNI routing protocol for mathematical support of packet switch.

Key words: satellite communication system, transport communication network, sustainability of communication, routing, ATM, PNNI.

Information about Author

Mikhailov Roman Leonidovich – Doctoral Candidate. The postgraduate student of the Department of Networks and Communication Systems of Space Systems. Mozhaisky Military Space Academy. Field of research: sustainability of communication, routing of data flow, unified influence of monitoring and rejection means on communication networks. Tel.: +7 911 777 69 73. E-mail: mikhailov-rom2012@yandex.ru

Address: Russia, 197198, Saint-Petersburg, Zhdanovskaya str., 13.

УДК 004.056

Уязвимости алгоритма вычисления секретного ключа в криптосистеме RSA

Алексеев А. П.

Постановка задачи: во многих публикациях отмечается, что неверный выбор параметров шифра RSA может привести к уменьшению его криптостойкости. В некоторых случаях открытый и закрытый ключи могут полностью совпасть и тогда абонент случайно опубликует секретный ключ. **Целью работы** является доказательство возможности формирования ключей близнецов, когда открытый и закрытый ключ полностью совпадают. **Используемые методы:** возможность формирования ключей близнецов теоретически обоснована с помощью восьми лемм. Наличие ключей близнецов подтверждено проведёнными расчётами с помощью математической системы Mathcad. При проведении расчётов были рассмотрены функции Эйлера, кратные десяти, и открытые экспоненты, которые оканчивались цифрами 1 и 9. **Новизна:** показано, что при значениях функции Эйлера, кратных десяти, существует вероятность открытой публикации секретного ключа, если открытая экспонента оканчивается на цифры 1 или 9. Функция Эйлера формируется кратная десяти, если хотя бы одно простое число оканчивается единицей. **Результат:** расчётным путём подтверждена возможность формирования ключей близнецов. **Практическая значимость:** полученные результаты позволяют повысить криптостойкость шифра RSA путём проверки на совпадение сформированных открытых и закрытых ключей и тем самым предотвратить атаку на ключи близнецы.

Ключевые слова: асимметричная криптосистема RSA, уязвимость, секретный ключ, открытый ключ, функция Эйлера, лемма, простое число, чётное число, нечётное число, числа Ферма.

Актуальность

Криптосистему RSA разработали R. Rivest, A. Shamir, L. Adleman [1], а саму концепцию шифрования с помощью открытого ключа предложили W. Diffie и M. Hellman [2].

Асимметричная криптосистема RSA широко используется в современных инфокоммуникационных системах благодаря своим несомненным достоинствам. Положительными свойствами этой криптосистемы являются возможность передачи приватной информации по незащищённым каналам связи без предварительной передачи секретных ключей с помощью курьеров [3] и обеспечение цифровой подписи финансовых документов [4]. На базе RSA реализована известная почтовая программа PGP [5]. Многие фирмы выпускают микросхемы, которые аппаратно реализуют криптосистему RSA [7].

Постановка задачи

В работах [9, 10] отмечается, что для формирования ключей необходимо использовать простые числа, длины которых должны быть примерно одинаковые. Для предотвращения факторизации модуля разрядность простых чисел в настоящее время должна быть не менее 1024...4096 бит [8, 10].

В ряде публикаций отмечается, что недопустимо использовать открытую экспоненту малой разрядности [10, 14]. При формировании открытой экспоненты из множества допустимых значений рекомендуют формировать её по случайному закону [7, 11, 13]. В некоторых источниках предлагают

использовать открытые экспоненты, которые содержат малое число единиц при их представлении в двоичной системе счисления [7], например, 3, 17, 65537. Это позволяет повысить скорость шифрования, так как уменьшается число операций возведения в степень. В других источниках рекомендуют использовать числа Мерсенна, Ферма [6] и малые нечётные числа [10, 12].

Использование некоторых из перечисленных рекомендаций может привести к появлению уязвимостей в криптосистеме RSA. Взлом криптосистемы возможен путём проведения атаки на наличие ключей близнецов.

Теоретическое обоснование

Известно, что расчёт секретной экспоненты t в криптосистеме RSA осуществляется с помощью сравнения [1]:

$$s \cdot t \equiv 1(\text{mod}(\varphi(r))), \quad (1)$$

здесь s – число взаимно простое с $\varphi(r)$, так называемая открытая экспонента; r – произведение двух простых чисел p и q (модуль); $\varphi(r)$ – функция Эйлера, которая вычисляется по формуле:

$$\varphi(r) = (p-1) \cdot (q-1). \quad (2)$$

Из соотношения (1) по вычисленному значению функции Эйлера $\varphi(r)$ и выбранному значению s требуется найти такое значение t , при котором целочисленное деление величины $s \cdot t$ на $\varphi(r)$ даст остаток 1.

Для проведения анализа уязвимостей криптосистемы RSA рассмотрим несколько лемм.

Лемма 1.

Функция Эйлера $\varphi(r)$ является чётным числом.

Доказательство.

Функция Эйлера вычисляется по формуле (2). Все простые числа, используемые в криптографии, нечётные, поэтому функция Эйлера, равная произведению двух чётных чисел, является чётным числом.

Лемма 2.

Множество чисел открытой экспоненты s состоит из множества нечётных чисел.

Доказательство.

В соответствии с алгоритмом формирования ключей для асимметричной криптосистемы RSA числа s должны быть взаимно простыми с чётными числами $\varphi(r)$ [1], поэтому числа s будут обязательно нечётными.

Лемма 3.

Секретная экспонента t является нечётным числом.

Доказательство.

В соответствии с выражением (1) целочисленное деление произведения $s \cdot t$ на чётное число $\varphi(r)$ должно дать остаток, равный единице. Это возможно только при нечётных значениях произведения $s \cdot t$. В соответствии с леммой 2 число s является нечётным. Произведение $s \cdot t$ будет нечётным только при нечётных значениях t .

Лемма 4.

Функция Эйлера кратна 10, если хотя бы одно простое число модуля (p или q) оканчивается на 1.

Доказательство.

Используемые в практической криптографии простые числа могут оканчиваться только цифрами 1, 3, 7 и 9. Единственное простое число, которое оканчивается на 5 – это само число 5. Однако оно слишком мало для формирования реальных криптографических ключей. В соответствии с формулой для вычисления функции Эйлера (2) произведение указанных сомножителей будет кратно 10, если хотя бы одно простое число оканчивается на 1.

Считая, что формирование простых чисел происходит по случайному закону, можно ожидать, что 40% ключей создаётся при значениях функции Эйлера, кратной 10.

Лемма 5.

Если $\varphi(r)$ кратно 10, а число s оканчивается цифрой 7, то число t оканчивается цифрой 3.

Доказательство.

Так как произведение указанных чисел s и t будет оканчиваться единицей, то в результате вычитания единицы из произведения $s \cdot t$ будет получено число, кратное 10.

Таким образом, величину t нужно искать среди чисел, у которых последняя цифра 3, например, 3, 13, 23 и т.д.

Пример 1.

Пусть $\varphi(r) = 440$, $s = 27$. Расчёт секретного ключа с помощью обобщённого алгоритма Евклида [12] дал $t = 163$.

Лемма 6.

Если $\varphi(r)$ кратно 10, а число s оканчивается цифрой 3, то число t оканчивается цифрой 7.

Доказательство.

Доказательство аналогично доказательству леммы 5.

Итак, величину t нужно искать среди чисел, оканчивающихся на цифру 7, например, 7, 17, 27 и т.д.

Пример 2.

Пусть $\varphi(r) = 440$, $s = 23$, тогда $t = 287$.

Лемма 7.

Если $\varphi(r)$ кратно 10, а s оканчивается цифрой 9, то последняя цифра числа t должна быть 9.

Доказательство.

Только произведение двух чисел, оканчивающихся цифрами 9 (при s , оканчивающимся на 9), даёт число, у которого последняя цифра 1. В этих случаях число $s \cdot t - 1$ будет кратно 10.

Пример 3.

Пусть $\varphi(r) = 120$, $s = 19$. Расчёт дал $t = 19$.

Лемма 8.

Если $\varphi(r)$ кратно 10, а s оканчивается цифрой 1, то последняя цифра числа t должна быть 1.

Доказательство.

Только произведение двух чисел, оканчивающихся цифрами 1 (при числе s , оканчивающемся цифрой 1), даёт число, у которого последняя цифра 1. В этих случаях число $s \cdot t - 1$ будет кратно 10.

Пример 4.

Пусть $\varphi(r) = 120$, $s = 31$. Расчёт дал $t = 31$.

Леммы 7 и 8 указывают на снижение криптостойкости в рассмотренных случаях (последние цифры открытого и закрытого ключей обязательно совпадают). Можно предположить, что могут быть сформированы полностью совпадающие числа s и t (ключи близнецы), то есть секретный ключ может быть ошибочно опубликован абонентом. Примеры 3 и 4 подтверждают это утверждение.

Другими словами, при $\varphi(r)$ кратном десяти и открытых экспонентах, оканчивающихся цифрами 1 и 9 есть вероятность открытой публикации секретного ключа. Если величина s выбирается по случайному закону, то для $\varphi(r)$, кратных 10, вероятность формирования экспонент, оканчивающихся цифрами 1 или 9, составляет 0,2 (половина всех ключей, у которых функция Эйлера кратна десяти). При этом небольшая часть секретных ключей полностью совпадёт с открытыми ключами.

Экспериментальная проверка

Рассмотренная гипотеза о возможности совпадения открытых и закрытых ключей была проверена расчётным путём с помощью математической системы Mathcad 15. Программа для расчёта ключей приведена в Приложении 1. Для $\varphi(r)=440$ выявлено 15 уязвимостей (открытый и закрытый ключи полностью совпали, например, 241, 351, 309, 419). Для $\varphi(r)=18240$ выявлено также 15 ключей близнецов (например, 14401, 14591, 15391). В последнем случае анализировались только ключи, оканчивающиеся на единицу.

Расчёты проводились следующим образом. Выбирались простые числа, которые оканчивались цифрой 1 (в этом случае функция Эйлера будет кратна 10). Для выбранного значения функции Эйлера определялись все допустимые значения открытой экспоненты s . Для значений s , которые оканчивались цифрами 1 или 9, вычислялись секретные экспоненты t . Отмечались совпадающие значения s и t .

Фрагмент протокола выполненных вычислений приведён в таблице 1.

Таблица 1. Фрагмент протокола вычислений

$\phi(r)$	s	t	$\phi(r)$	s	t	$\phi(r)$	s	t
440	21	21	18240	191	191	120	11	11
440	111	111	18240	2431	2431	120	31	31
440	131	131	18240	3041	3041	120	61	61
440	221	221	18240	5281	5281	120	71	71
440	241	241	18240	5471	5471	120	91	91
440	331	331	18240	6271	6271	120	101	101
440	351	351	18240	8321	8321			
440	89	89	18240	9121	9121			
440	109	109	18240	9311	9311			
440	199	199	18240	11551	11551			
440	219	219	18240	12161	12161			
440	309	309	18240	14401	14401			
440	329	329	18240	14591	14591			
440	419	419	18240	15391	15391			
440	439	439	18240	17441	17441			

Выводы

При практическом формировании ключей в криптосистеме RSA в случаях, когда функция Эйлера кратна 10, а открытая экспонента оканчивается цифрами 1 или 9, следует произвести проверку на полное совпадение сформированных открытого и закрытого ключей. Очевидно, что совпадающие ключи не должны быть использованы.

Для исключения возникновения ключей близнецов при формировании открытой экспоненты нужно использовать числа, которые оканчиваются на 3 или 7, например, простые числа Ферма 17, 257, 65537.

Определить теоретически число ключей близнецов не представляется возможным. Выполненный объём вычислений в настоящее время мал, поэтому пока невозможно точно определить вероятность возникновения ключей близнецов. Их число нетривиально зависит от значения функции Эйлера. В настоящее время известна только верхняя граница вероятности появления одинаковых ключей (не более 0,2). Отсутствие оценки вероятности возникновения ключей близнецов объясняется необходимостью разработки соответствующего программного обеспечения и большим временем счёта. Если используются 1024-х битные простые числа, то число возможных функций Эйлера оценивается величиной $3,2 \cdot 10^{616}$. Для получения статистически устойчивого результата нужна репрезентативная выборка. Понятно, что время счёта будет внушительным. Однако предотвратить формирование ключей близнецов легко. Для этого достаточно произвести сравнение открытой и закрытой экспонент. Основная цель данной работы показать наличие ключей близнецов. В дальнейшем предстоит получить количественную оценку вероятности их формирования и оценить, насколько имеющееся ограничение уменьшит пространство допустимых ключей.

Приложение 1.

Программа на языке Mathcad 15 для формирования открытой и закрытой ЭКСПОНЕНТ

Mathcad 15

Выбор простых чисел

$p1 := 97$ $q1 := 191$

Расчет функции Эйлера

$r1 := p1 \cdot q1$ $r1 = 18527$

$w1 := r1 - p1 - q1 + 1$

$w1 = 18240$

Расчет взаимно простых чисел

$ORIGIN := 1$

$\text{nod}(a,b) := \begin{cases} \text{while } (a \neq 0) \wedge (b \neq 0) \\ \quad \text{if } a \geq b \\ \quad \quad a \leftarrow \text{mod}(a,b) \\ \quad \quad 0 \\ \quad \text{otherwise} \\ \quad \quad b \leftarrow \text{mod}(b,a) \\ \quad \quad 0 \\ \text{nod} \leftarrow a + b \\ \text{nod} \end{cases}$	$\text{pr}(a) := \begin{cases} \text{for } i \in 2..a \\ \quad \text{if } \text{nod}(i,a) = 1 \\ \quad \quad j \leftarrow j + 1 \\ \quad \quad d_j \leftarrow i \\ \quad 0 \\ d \end{cases}$
---	--

Взаимно простые числа

		1
1		7
2		11
$\text{pr}(18240) =$	3	13
	4	17
	5	23
	6	...

Обобщенный алгоритм Евклида

a - функция Эйлера; b - открытая экспонента

$a := 18240$ $b := 14591$

$$U := \begin{pmatrix} \overrightarrow{a} \\ 1 \\ 0 \end{pmatrix} \quad V := \begin{pmatrix} \overrightarrow{b} \\ 0 \\ 1 \end{pmatrix} \quad T := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

```
k1(a,b) := while  $T_1 \neq 0$ 
     $c \leftarrow \frac{U_1}{V_1}$ 
     $q \leftarrow \text{floor}(c)$ 
     $T_1 \leftarrow \text{mod}(U_1, V_1)$ 
     $T_2 \leftarrow U_2 - q \cdot V_2$ 
     $P \leftarrow T_3$ 
     $P \leftarrow P + a \text{ if } P < 0$ 
     $T_3 \leftarrow U_3 - q \cdot V_3$ 
     $U \leftarrow V$ 
     $V \leftarrow T$ 
P
```

t1 - секретная экспонента

t1 := k1(a,b) t1 = 1.4591×10^4

Литература

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. 1978. Т. 21. № 2. Pp. 120-126.
2. Diffie W., Hellman M. New Directions in Cryptography // IEEE Trans. Inform. Theory IT-22, (Nov. 1976). Pp. 644-654.
3. Алексеев А. П., Орлов В. В. Стеганографические и криптографические методы защиты информации. Самара: ИУНЛ ПГУТИ, 2010. 330 с.
4. Алексеев А. П. Информатика для криптоаналитиков. Самара: ИУНЛ ПГУТИ, 2015. 376 с.
5. Алексеев А. П. Информатика 2015. М.: СОЛОН-Пресс, 2015. 400 с.
6. RSA // Википедия, свободная энциклопедия [Электронный ресурс], 2015. URL: <https://ru.wikipedia.org/wiki/RSA.html> (дата обращения 1.08.2015).
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002. 816 с.
8. Сمارт Н. Криптография. М.: Техносфера, 2006. 528 с.
9. Введение в криптографию / Под общей редакцией Яценко В.В. Спб.: Питер, 2001. 288 с.
10. Фергюсон Н., Шнайер Б. Практическая криптография. М.: Издательский дом «Вильям», 2005. 424 с.
11. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.
12. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2010. 232 с.
13. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.

14. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М.: ДМК, 2000. 448 с.

References

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 1978. vol. 21. no. 2, pp. 120-126.
2. Diffie W., Hellman M. New Directions in Cryptography. *IEEE Trans. Inform. Theory IT-22*, 1976, pp. 644-654.
3. Alekseev A. P., Orlov V. V. *Steganograficheskie i kriptograficheskie metody zashchity informatsii* [Steganographic and Cryptographic Methods of Information Protection]. Samara, IUNL PGUTI Publ., 2010. 330 p. (in Russian).
4. Alekseev A.P. *Informatika dlya kriptoanalitikov*. [Informatics for Cryptanalysts]. Samara, IUNL PGUTI Publ., 2015. 376 p. (in Russian).
5. Alekseev A. P. *Informatika 2015* [Informatics 2015]. Moscow, SOLON-Press Publ., 2015. 400 p. (in Russian).
6. RSA. *Vikipediya* [RSA. Wikipedia, the free Encyclopedia]. Available at: <https://ru.wikipedia.org/wiki/RSA> (Accessed 1 August 2015).
7. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, John Wiley & Sons, Inc. Publ. 792 p. 1996.
8. Smart N. *Cryptography: An Introduction*. New York, McGraw-Hill Companies Publ., 433 p. 2004.
9. Jashhenko V. V. *Vvedenie v kriptografiju* [Introduction to Cryptography]. Sankt Peterburg, Piter Publ., 2001. 288 p. (in Russian).
10. Ferguson N., Schneier B. *Practical Cryptography*. New York, JohnWiley&Sons Publ., 432 p. 2003.
11. Alferov A. P., Zubov A. Ju., Kuzmin A. S., Cheremushkin A. V. *Osnovy kriptografii* [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2002. 480 p. (in Russian).
12. Rjabko B. Ja., Fionov A. N. *Osnovy sovremennoj kriptografii i steganografii* [The Foundations of Modern Cryptography and Steganography]. Moscow, Gorjachaja linija-Telekom Publ., 2010. 232 p. (in Russian).
13. Romanec Ju. V., Timofeev P. A., Shangin V. F. *Zashhita informacii v kompjuternyh sistemah i setjah* [Protecting Information in Computer Systems and Networks]. Moscow, Radio i svjaz Publ., 2001. 376 p. (in Russian).
14. Petrov A. A. *Kompjuternaja bezopasnost. Kriptograficheskie metody zashhity* [Computer Security. Cryptographic Methods of Protection]. Moscow, DМК Publ., 2000. 448 p. (in Russian).

Статья поступила 9 августа 2015 г.

Информация об авторе

Алексеев Александр Петрович - кандидат технических наук, доцент, старший научный сотрудник. Профессор кафедры информатики и вычислительной техники. Поволжский государственный университет телекоммуникаций и информатики. Область научных интересов: криптография; стеганография; информатика; контрольно-измерительная техника; дефектоскопия. Тел.: +7(846)228 00 57. E-mail: apa_ivt@rambler.ru

Адрес: 443013, г. Самара, ул. Льва Толстого, 23.

Vulnerabilities Algorithm for Computing the Secret Key in the RSA Cryptosystem

Alekseev A. P.

Purpose. In many publications indicates that the wrong choice of parameters RSA encryption may reduce the reliability of his. However, no mention of the fact that the public key and private key, in some cases, can completely match the subscriber and then publish the private key. The aim is to prove the possibility of forming twin keys where public and private keys are the same. **Methods.** The possibility of forming the twin keys theoretically justified with eight lemmas. **Novelty.** It is shown that for values of Euler's function, a multiple of ten, there is a possibility of publication of the private key, if the public key numbers ending in 1 or 9. **Results.** By calculation confirmed the possibility of the formation of the twin keys. **Practical relevance.** The results will improve RSA cryptographic cipher by checking for a match generated public and private keys.

Key words: asymmetric cryptosystem RSA, vulnerability, private key, public key, Euler function, Lemma, a prime number, an even number, odd number, the number of Farms.

Information about Author

Alekseev Aleksandr Petrovich - Ph.D. of Engineering Sciences, Associate Professor, Senior Research Officer. Professor at the Department of Computer Science and Engineering. Povolzhye State University of Telecommunications and Informatics. Field of research: cryptography; steganography, computer science; testing and measuring equipment; flaw detection. Tel.: +7(846)2280057. E-mail: apa_ivt@rambler.ru

Address: Russia, 443013, Samara, L. Tolstogo Street, 23.

УДК 004.72

Анализ качества обслуживания в воздушно-космической сети связи на основе иерархического и децентрализованного принципов ретрансляции информационных потоков

Аганесов А. В.

Постановка задачи. Создание объединенных воздушно-космических сетей связи актуализирует вопросы решения задач маршрутизации и ретрансляции сообщений в них. При этом необходимо обеспечить заданное качество обслуживания трафика. В более ранних работах автора рассмотрены два варианта структуры воздушно-космической сети. Первый – иерархический, когда все информационные потоки воздушных сетей ретранслируются через космическую сеть. Второй вариант предусматривает дополнительно объединение воздушных сетей по Mesh-технологии и децентрализованную ретрансляцию части трафика по смежным воздушным сетям. **Целью работы** является сравнительный анализ оценки качества обслуживания в этих вариантах структуры воздушно-космической сети по показателям пропускной способности. **Используемые методы.** В основу модели воздушно-космической сети положены ранее опубликованные работы автора в которых представлены модели иерархической и децентрализованной ретрансляции информационных потоков в воздушно-космической сети. При этом модель воздушной сети строится на основе модели протокола CSMA/CA, а модель спутниковой сети – на основе модели протокола S-Aloha. **Новизна.** Элементом новизны представленной работы является используемые оригинальные модели и впервые проведенные сравнительные оценки пропускной способности воздушно-космической сети при иерархической и децентрализованной ретрансляции информационных потоков. **Практическая значимость:** представленные оценки пропускной способности в дальнейшем предполагается использовать для обоснования принципов ретрансляции информационных потоков мультимедийных данных в глобальных воздушно-космических сетях. Планируется использовать результаты исследований для разработки математического обеспечения маршрутизаторов абонентов воздушно-космических сетей связи, построенных с использованием Mesh-технологий. Так же возможна реализация на основе протокола OpenFlow для программно-конфигурируемых сетей SDN.

Ключевые слова: сеть связи, ретрансляция, маршрутизация, сеть спутниковой связи, сеть воздушной радиосвязи, S-Aloha, CSMA.

Актуальность

В настоящее время в соответствии с перспективной концепцией построения систем связи специального назначения предполагается переход к много эшелонированному принципу построения объединенных систем связи Вооруженных сил (ВС). При этом при построении систем связи предполагается в максимальной степени задействовать коммерческие и открытые стандарты и протоколы.

Как показал анализ современных технологических решений по построению систем связи [1-3] в основу также воздушных сетей радиосвязи будут положены радиосети, реализованные на основе протоколов случайного множественного доступа и в перспективе объединяемые в единое информационное пространство за счет использования Mesh-технологий [4-6]. Ретрансляция сообщений между отдельными сетями, потребует создания новых технологических решений по обеспечению Mesh-ретрансляции информационных потоков. Для обеспечения заданного качества обслуживания пользовательского трафика в объединенной сети связи требуется выработать

единые протоколы ретрансляции информационных потоков. Данная задача особенно актуальна для сетей воздушной радиосвязи (СВРС) в УКВ диапазоне, для которых предусматривается объединение через сети спутниковой связи (ССС). Такое объединение дополнительно обусловлено тем, что именно на СВРС, в условиях проведения военной операции, планируется возложить информационное обеспечение авиации и ретрансляцию информационных потоков от подразделений сухопутных войск, и от развертываемых в районе операции разведывательных сетей на основе БПЛА. С одной стороны это позволяет обеспечить глобальность управления авиацией, а с другой стороны – актуализирует вопросы ретрансляции информационных потоков в такой объединенной воздушно-космической сети (ВКСС). При этом отличительной особенностью ВКСС является то, что ее элементы, как показано в работах [7-12], доступны наземным и авиационным средствам радиоэлектронного подавления (РЭП), что существенно затрудняет ретрансляцию информационных потоков, а также снижает эффективность протоколов маршрутизации в сети.

Анализ современных технических решений на основе работ [1-3] показал, что в основу воздушного эшелона будет положены системы обмена данными (СОД) в интересах которых, за счет перспективных средств и комплексов связи, будут развернуты отдельные СВРС обеспечивающие высокоскоростной цифровой информационный обмен. СОД будут обладать высокой совместимостью с наземными средствами радиосвязи и обеспечивать бесшовную ретрансляцию информационных потоков. В таблице 1 приведены основные характеристики существующих и разрабатываемых систем обмена данными по материалам из [1]. В настоящее время получила широкое применение СОД на базе ТКС-2 (ТКС-2М), однако наибольшей эффективностью обладает система ОСНОД, которая в настоящее время планируется к использованию в перспективных СВРС.

Таблица 1 – Характеристики систем обмена данными [1]

№	Характеристики	ТКС-2 (ТКС-2М)	ОСНОД
1	Назначение	Типовой комплекс связи для обмена телекодированной информацией	Объединенная система связи, обмена данными, навигации и опознавания
2	Виды сетей обмена данными	СОД между самолетами, между ПУ и самолетами	Сеть обмена всеми видами информации между АК, между АК и ПУ, между ПУ
3	Возможность закрытия	Есть	Есть
4	Количество абонентов	20	1800
5	Объем сообщения, бит	1024	1024, 2048
6	Возможность автоматической ретрансляции сообщений	Есть	Есть
7	Диапазон частот	ДКМВ, МВ-ДМВ	ДМВ

* ТКС-2М отличается от ТКС-2 циклограммой работы и составом передаваемой информации.

Технической основой перспективных СОД воздушного эшелона станет, комплекс связи С-111, который не только обеспечит летательные аппараты (ЛА) фронтовой, истребительной и армейской авиации высокоскоростной цифровой связью, но и будет использоваться совместно с наземными подразделениями сухопутных войск. Для этого в радиостанциях комплекса связи предусмотрен режим помехозащищенной связи ППРЧ-Б [8].

ТТХ комплекса связи С-111, значимые для решения задач ретрансляции информационных потоков представлены в таблице 2 по данным работ [1, 3, 13]. Как показывает анализ данных таблицы 2, в состав комплекса авиационной связи включена станция спутниковой связи, которая позволит организовать сопряжение СОД через ССС. Концепцией построения систем связи специального назначения предполагается, что ССС будет использовать режим коммутации пакетов с их обработкой на борту [14, 15]. При этом спутники-ретрансляторы (СР) будут использоваться для иерархического «роуминга» информационных потоков передающихся между различными воздушными и наземными полевыми радиосетями, имеющих различную войсковую и ведомственную принадлежность или не имеющих прямой электромагнитной доступности, но оснащенные средствами спутниковой связи «Багет-К», «Ливень», «Легенда» и др. со скоростями до 2,4 кбит/с (а при переходе к ЕССС-3 – до 2 Мбит/с) [3]. При этом в составе ССС для организации такого «роуминга» предполагается использовать каналы и частотные диапазоны отводимые под функционирование подвижных ССС, а организацию доступа абонентов воздушных и наземных полевых сетей к СР производить по протоколу случайного множественного доступа S-Aloha.

Таблица 2 – Некоторые ТТХ перспективного комплекса связи

№	Характеристика	Значение
1	Скорости передачи данных, кбит/с: - ДКМВ - МВ-ДМВ - ОСНОД (эффект.) - СМВ - спутниковая линия связи ЕССС-2 (ЕССС-3) ДМВ-2	до 2,4 до 16 до 40 (100) до 34 400 до 2,4 (до 2048)
2	Количество одновременно обслуживаемых сетей	до 38
4	Направлений связи: - ДКМВ - МВ-ДМВ - ОСНОД (эффект.) - СМВ - спутниковая линия связи ЕССС-2 (ЕССС-3) ДМВ-2	1 2 1 1 1
5	Дальность связи, км: - в направлении «земля-борт» для ДКМВ - в направлении «земля-борт» для МВ-ДМВ, ОСНОД - в направлении «борт-борт» для МВ-ДМВ, ОСНОД	1500 350 500

Таблица 3 - Допустимые значения параметров качества обслуживания при передаче мультимедийного трафика [16, 17]

Тип сервиса	Параметры качества обслуживания				
	Время установления соединения, с	Вероятность разрыва соединения	Задержка, мс	Джиттер, мс	Вероятность потери данных
IP-телефония	0,5-1	10^{-3}	25-500	100-150	10^{-3}
Видеоконференция	0,5-1	10^{-3}	30	30-100	10^{-3}
Цифровое видео по запросу	0,5-1	10^{-3}	30	30-100	10^{-3}
Передача данных	0,5-1	10^{-6}	50-1000	-	10^{-6}
Телевизионное вещание	0,5-1	10^{-8}	1000	-	10^{-8}

Таблица 4 - Требования к качеству услуг, предоставляемых мультисервисными сетями связи [16, 17]

Тип данных	Название услуги	Требуемая скорость передачи	Параметры качества услуги		
			Задержка, мс	Джиттер	Потери, %
Аудио	Телефония	4-64 кбит/с	<150 мс (отличное QoS); <400 мс (допустимое QoS)	<1 мс	<3%
	Передача голоса	4-32 кбит/с	<1 с (для воспроизведения); <2 с (для записи)	<1 мс	<3%
	Звуковое вещание	16-128 кбит/с	<10 с	<<1 мс	<1%
Видео	Видео-конференция	>384 кбит/с	<150 мс (отличное QoS); <400 мс (допустимое QoS)		<1%
Данные	Просмотр WEB-страниц	□ 10 кБ	<2 с/стр. (отличное QoS); <4 с/стр. (допустимое QoS)	-	0
	Передача файлов	10 кБ – 10 МБ	<15с (отличное QoS); <60 с (допустимое QoS)	-	0
	Передача изображений	100 кБ	<15с (отличное QoS); <60 с (допустимое QoS)	-	0
	Доступ к электронной почте	<10 кБ	<2 с (отличное QoS); <4 с (допустимое QoS)	-	0
	Факс	□ 10 кБ	<30с/ стр.	-	< 10^{-6} BER

Информационный обмен внутри СВРС и ССС будет вестись с помощью универсальных кодограмм – УКВС, которые в зависимости от длины сообщения состоят из 1-го, 2-ух, 3-ех или 4-ех блоков по 256 бит в каждом блоке, то есть составляют сообщения объемом 256, 512, 768 и 1024 бит. При этом на максимальное время доставки УКВС накладываются ограничения, связанные с режимом реального времени управления авиацией и необходимостью передачи информационного трафика критичного к задержкам (речь, видео). Несмотря на то, что существующие стандарты передачи

информационных сообщений военного управления определяют граничные значения времени доведения в несколько секунд, к сообщениям голосового управления, а также к трафику фото и видео данных, поступающих от разведывательных средств на БПЛА в режиме реального времени, предъявляются гораздо более жесткие требования, обусловленные используемым кодеком информации (таблицы 3, 4) [16, 17].

Вышеуказанные факторы определяют актуальность разработки научно-методического обеспечения ретрансляции трафика СВРС через ССС в составе ВКС.

Анализ вариантов технологических решений по сопряжению отдельных сетей воздушной радиосвязи через сеть спутниковой связи

В настоящее время СВРС могут быть сопряжены через ССС за счет использования средств спутниковой связи «Багет-К», «4РТ-С», «Кулон-В» (таблица 5) [3].

Станция «Кулон-В» является первой самолетной станцией с пропускной способностью до десяти помехозащищенных каналов. Выполняет функции малоканальной или микроузловой земной станции (ЗС) космической связи, работающей в оперативно-тактических сетях связи. Применяемые в станции антенные синфазные решетки позволяют существенно улучшить аэродинамику самолета по сравнению с использованием параболической антенны. Станция позволяет организовать круглосуточную непрерывную связь на всей территории Северного полушария Земли [3].

Станция «Багет-К» предназначена для обеспечения в режиме реального времени самолетов ВВС и ВМФ дальней помехозащищенной засекреченной телефонной и телекодовой радиосвязью с наземными и корабельными пунктами управления через СР на стационарных и эллиптических орбитах Единой системы спутниковой связи. Устанавливается на самолетах типа Ту-160 [3].

Станция «4РТ-С» обеспечивает прием и передачу телекодовой и телеграфной информации в через СР на высокой эллиптической орбите Единой системы спутниковой связи [3].

Таблица 5 - Некоторые ТТХ авиационных средств спутниковой связи [3]

	Кулон-В	Багет-К	4РТ-С
Диапазон частот, ГГц	4/6	0,3/0,4	4/6
Дальность связи, км	до 17 000	до 17 000	до 17 000
Количество каналов связи:			
- телефонные	8×1,2 кбит/с	2×1,2 кбит/с	-
- телеграфные	6×0,25 кбит/с	2×0,25 кбит/с	-

Средство спутниковой связи «Кулон-В» в рамках ЕССС-2 способно организовывать каналы до 2,4-9,6 кбит/с, однако при переходе на ЕССС-3 планируется увеличить скорости мобильных авиационных абонентов до

2 Мбит/с. Это позволит организовать полноценную маршрутизацию информационных потоков отдельных СВРС через ССС.

В настоящее время используемые в СВРС и ССС алгоритмы маршрутизации различны. С целью упрощения программно-аппаратных средств, в при построении интегрированной ВКСС целесообразно использовать одну универсальную схему выбора маршрута. В этом случае во всех сегментах сети будут рассчитываться одни и те же показатели, на базе которых и определяются оптимальные в выбранной метрике маршруты. Однако в настоящее время различные сегменты интегрированных сетей проектируются и изготавливаются различными производителями, что придает задаче маршрутизации в интегрированных ВКСС особую актуальность.

Таким образом, в целом схема сопряжения СВРС через ССС в рамках интегрированной ВКСС будет иметь вид представленный на рис. 1.

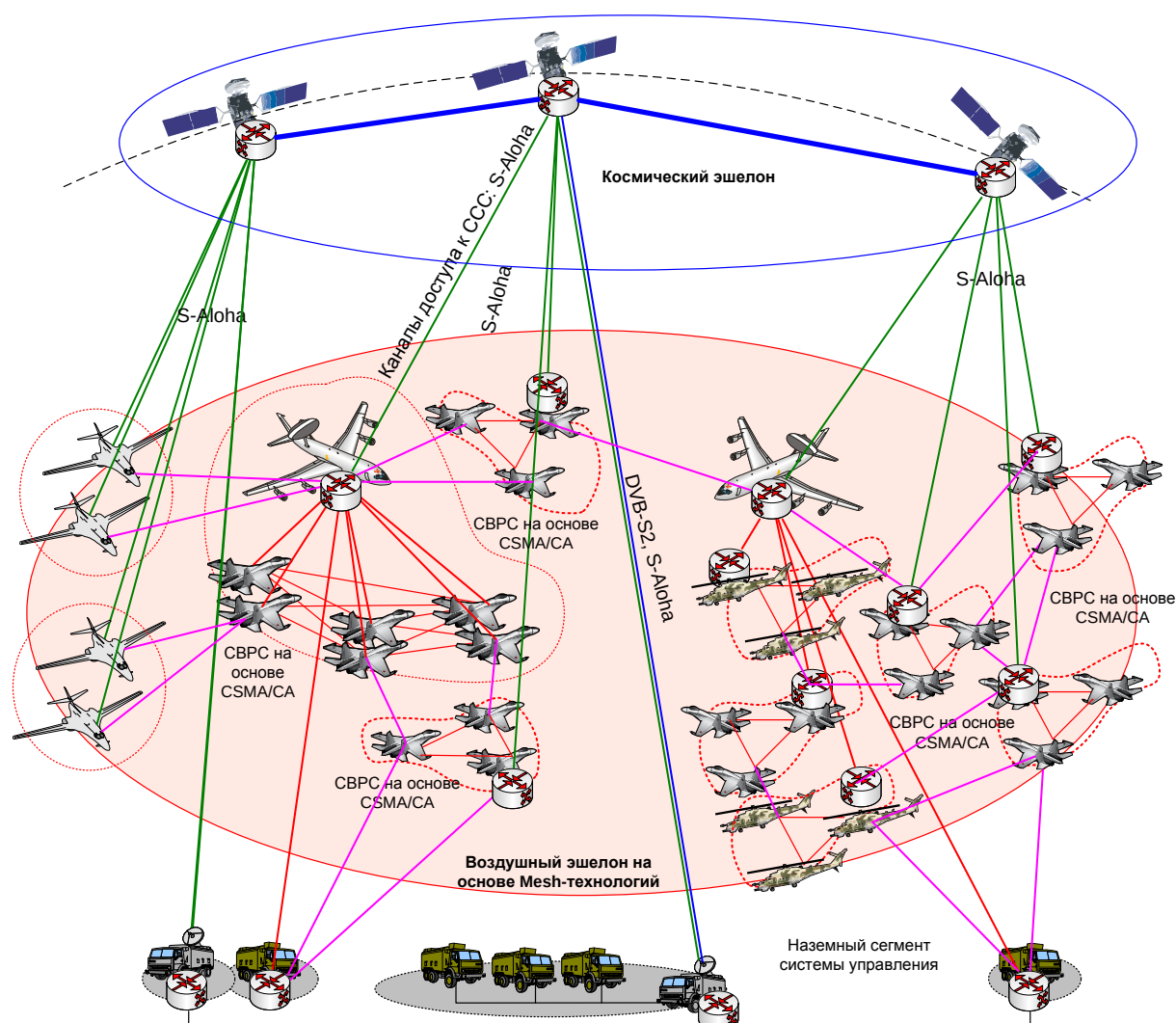


Рис. 1. Схема ВКСС на основе децентрализованного принципа ретрансляции информационных потоков

Как показано на рисунке, ССС предоставляет отдельным СВРС услуги глобальной транспортной сети, с помощью которой они сопрягаются между

собой, а также с наземной системой управления, кроме того отдельные СВРС могут объединяются между собой за счет использования Mesh-технологий. Подключение отдельных СВРС к ССС в рамках одного ствола СР ведется с помощью протокола случайного множественного доступа S-Aloha. Информационный обмен по межспутниковым радиолиниям, а также по каналам СР-шлюзовая станция ведется по стандарту DVB-S/S2.

В дальнейшем предлагается исследовать функционирование протоколов ретрансляции информационных потоков в ВКСС на основе централизованного (обмен СВРС между собой ведется через ССС) и децентрализованного принципа (обмен СВРС между собой ведется через ССС и через смежные СВРС объединенных на основе Mesh-технологий).

Постановка задачи анализ качества обслуживания в воздушно-космической сети связи на основе иерархического и децентрализованного принципов ретрансляции информационных потоков

Проведем анализ показателей качества ретрансляции информационных потоков в ВКСС по показателям:

- пропускная способность информационного направления связи;
- время задержки пакета в информационном направлении связи.

С учетом того, что ВКСС строится на основе:

- иерархического принципа информационного обмена (обмен СВРС между собой ведется через ССС);
- децентрализованного принципа информационного обмена (обмен СВРС между собой ведется через ССС и через смежные СВРС объединенных на основе Mesh-технологий).

Для формализации процесса информационного обмена в ВКСС введем следующие обозначения:

M – количество абонентов СВРС;

C – пропускная способность канала множественного доступа СВРС [бит/с];

$C_{ССС}$ – пропускная способность канала множественного доступа ССС [бит/с];

S – относительная пропускная способность канала множественного доступа СВРС, нормированная к C ;

$S_{ССС}$ – относительная пропускная способность канала множественного доступа ССС нормированная к $C_{ССС}$;

C_e – эффективная пропускная способность канала множественного доступа СВРС [бит/с];

$C_{e\ ССС}$ – эффективная пропускная способность канала множественного доступа ССС [бит/с];

$C_{e\ ИНС}$ – эффективная пропускная способность информационного направления связи (ИНС) [бит/с];

D_{mes} – объем пакета в СВРС [бит];

$D_{mes\ ССС}$ – объем пакета в ССС [бит];

$D_{mes\ ССС}$ – объем пакета в ССС [бит];

d_{max} – максимальный радиус сети СВРС [км];

d_{sot} – расстояние до спутника-ретранслятора (СР), образующего ССС [км].

Для низкоорбитальных ССС $d_{sot}=500..1500$ км, для геостационарных ССС $d_{sot}=40000$ км, для высокоэллиптических ССС $d_{sot}>40000$ км;

c – скорость распространения электромагнитных волн [км/с];

K – настойчивость протокола множественного доступа СВРС, определяемая как число попыток передачи пакета, в случае, если предыдущие попытки оканчиваются неудачей;

$K_{ССС}$ – настойчивость протокола множественного доступа S-Aloha, используемого в ССС;

λ – интенсивность трафика, поступающего от 1-го абонента в СВРС [бит/с];

$k_{вн}=0...1$ – коэффициент внешнего трафика СВРС, определяется как доля трафика СВРС передаваемого как через ССС, так и через смежные СВРС, объединенные по Mesh-технологии;

$k_{вн ССС}=0...1$ – коэффициент, определяющий долю внешнего трафика из СВРС в другую СВРС, передаваемого только через ССС;

$k_{кв}=0...1$ – коэффициент дополнительного трафика квитанций, определяется как доля от основного трафика содержания квитанции об успешном приеме пакета. Значение $k_{кв}=0,1$ соответствует случаю, когда на 10 пакетов основного трафика отправляется 1 пакет квитанции об их успешном приеме;

z – количество исходящих Mesh-каналов из СВРС в смежные СВРС;

$k_{св}=0...1$ – среднесетевой коэффициент связности СВРС со смежными СВРС по Mesh-каналам;

R – среднесетевое количество ретрансляций через СВРС, объединенных на основе Mesh-технологий, при доставке пакета из СВРС-источника в СВРС-получатель;

Λ – интенсивность трафика в СВРС без учета трафика квитанций об успешной доставке и внешнего трафика, поступающего в СВРС [бит/с];

$\Lambda_{ССС}$ – общая интенсивность трафика в ССС с учетом трафика квитанций об успешной доставке [бит/с]

$\Lambda_{СВРС}$ – общая интенсивность трафика в СВРС с учетом внешнего трафика и трафика квитанций об успешной доставке [бит/с];

$T_{зад}$ – задержка передачи пакета по n -ой СВРС [с];

$T_{зад ССС}$ – задержка передачи пакета по ССС [с];

$T_{зад ИНС}$ – задержка передачи пакета по ИНС [с].

Рамки исследования:

- протокол связи в СВРС – CSMA/CA;
- протокол связи в ССС – S-Aloha; при централизованном принципе ретрансляции - все СВРС соединены через ССС по принципу «звезды», причем каждая СВРС доступна из другой сети за один шаг ретрансляции через ССС;
- при централизованном принципе ретрансляции - все СВРС соединены через ССС по принципу «звезды», причем каждая СВРС доступна из

другой сети за один шаг ретрансляции через ССС, дополнительно все СВРС соединены между собой в соответствии с количеством исходящих Mesh-каналов;

- трафик представляет собой простейший пуассоновский поток событий, состоящих в поступлении отдельных пакетов.

Целью разработки модели является оценка временных параметров задержки передачи сообщений и пропускной способности ИНС в ВКСС, использующей децентрализованный принцип ретрансляции информационных потоков на основе Mesh-технологии.

Модель воздушно-космической сети связи

с иерархическим принципом ретрансляции информационных потоков

Рассмотрим ВКСС с иерархическим принципом информационного обмена (рис. 2). В данной сети все межсетевые ИНС «СВРС-СВРС» идут через ССС. В предыдущих работах автора получены аналитические соотношения для упрощенного моделирования такой сети, схема вывода которой представлена на рис. 3. При этом основными допущениями модели являются:

- информационный трафик, циркулирующий во всех СВРС имеет равную интенсивность Λ_1 ;
- все СВРС имеют одинаковые параметры объема пакета, радиуса сети, настойчивости протокола CSMA/CA равные соответственно - D_{mes} , d_{max} , K ;
- коэффициент внешнего трафика у всех СВРС одинаков и равен $k_{вн}$, причем внешний трафик равномерно распределен по СВРС и коэффициенты трафика по всем межсетевым направлениям $СВРС_i \rightarrow СВРС_j$ имеют равные значения: $k_{вн\ i,j} = k_{вн}/(N-1)$.

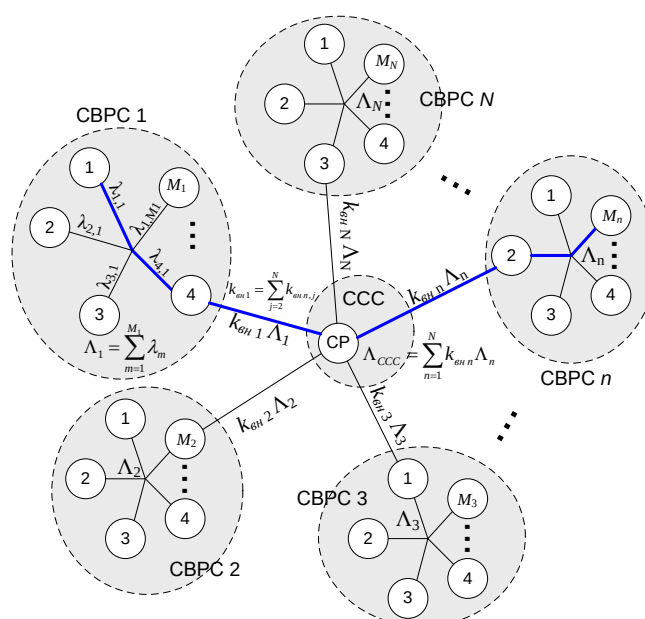


Рис. 2. Общая схема распределения интенсивностей информационного трафика циркулирующего в ВКСС без учета квитирувания

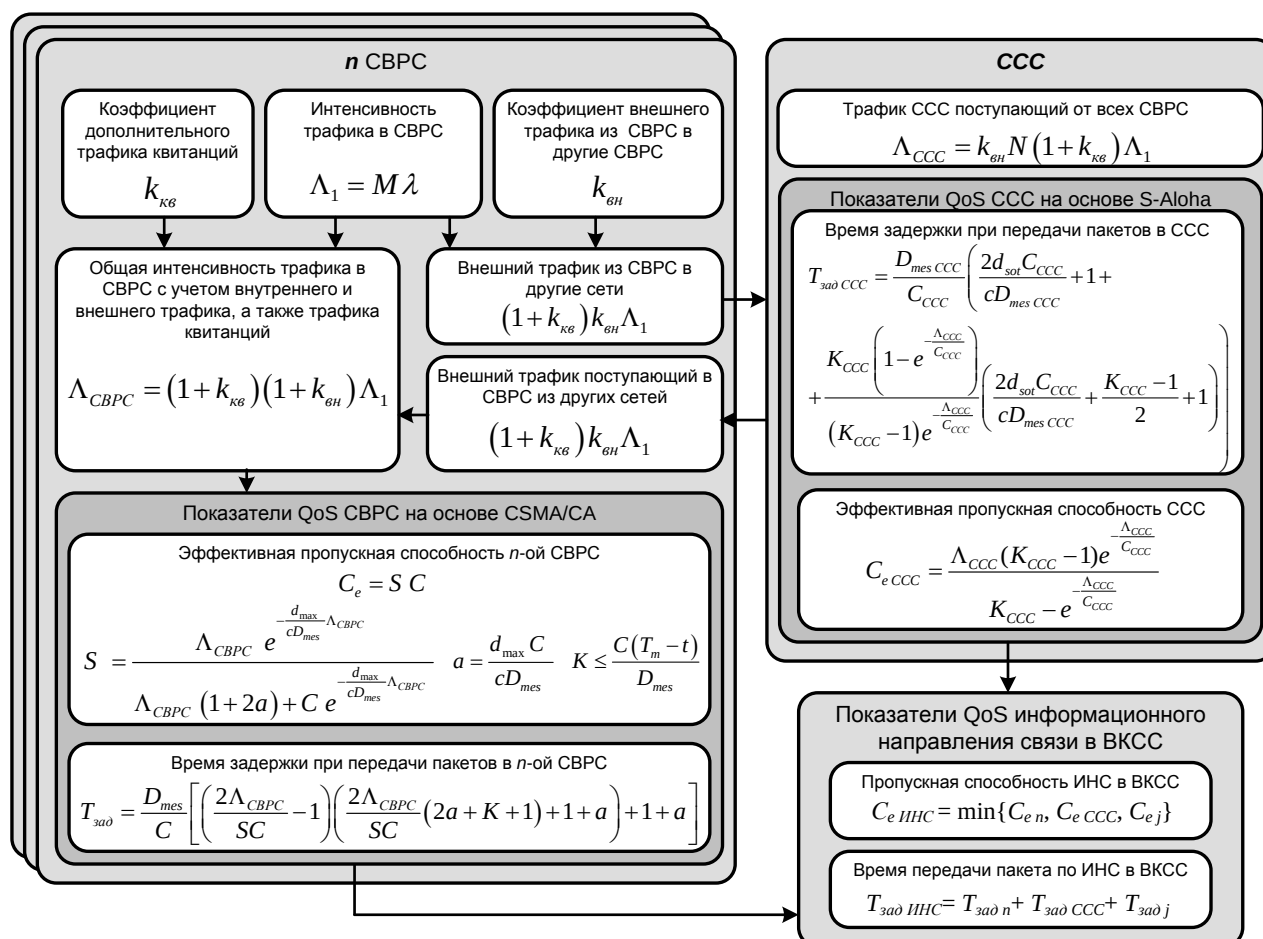


Рис. 3. Упрощенная схема аналитических вычислений для модели ВКСС с централизованным принципом информационного обмена

В соответствии со схемой информационного обмена (рис. 2) и схемой аналитических вычислений для модели ВКСС с иерархическим принципом информационного обмена (рис. 3) выражения для интенсивности трафика примут вид:

- интенсивность трафика циркулирующего в произвольной СВРС:

$$\Lambda_{СВРС} = (1 + k_{кв})(1 + k_{вн})\Lambda_1, \quad (1)$$

- интенсивность трафика в CCC:

$$\Lambda_{CCC} = k_{вн} N (1 + k_{кв}) \Lambda_1. \quad (2)$$

Общий вид ИНС в иерархической ВКСС представлен на рис. 4.

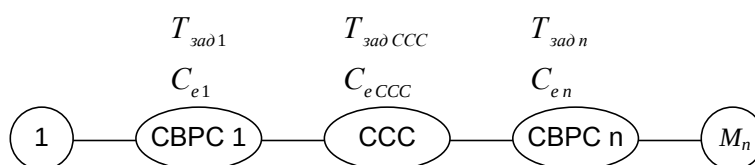


Рис. 4. Общая схема ИНС в ВКСС с иерархическим принципом информационного обмена

В ИНС, представленной на рис. 4, время задержки передачи пакета между абонентами n -ой и j -ой СВРС будет являться суммой задержек пакета на всех звеньях ИНС:

$$T_{\text{зад ИНС}} = 2T_{\text{зад}} + T_{\text{зад CCC}}. \quad (3)$$

При этом время задержки пакета при передаче по всем отдельным звеньям с учетом выражений (1) и (2) будет определяться как:

1) для СВРС на основе протокола CSMA/CA:

$$T_{\text{зад}} = \frac{D_{\text{mes}}}{C} \left[\left(\frac{2\Lambda_{\text{CBPC}}}{SC} - 1 \right) \left(\frac{2\Lambda_{\text{CBPC}}}{SC} (2a + K + 1) + 1 + a \right) + 1 + a \right], \quad (4)$$

$$\text{где: } S = \frac{\Lambda_{\text{CBPC}} e^{-\frac{d_{\text{max}}}{cD_{\text{mes}}} \Lambda_{\text{CBPC}}}}{\Lambda_{\text{CBPC}} (1 + 2a) + C e^{-\frac{d_{\text{max}}}{cD_{\text{mes}}} \Lambda_{\text{CBPC}}}}, \quad a = \frac{d_{\text{max}} C}{cD_{\text{mes}}}, \quad K \leq \frac{C(T_m - t)}{D_{\text{mes}}}.$$

2) для CCC на основе протокола S-Aloha:

$$T_{\text{зад CCC}} = \frac{D_{\text{mes CCC}}}{C_{\text{CCC}}} \left(\frac{2d_{\text{сot}} C_{\text{CCC}}}{cD_{\text{mes CCC}}} + 1 + \frac{K_{\text{CCC}} \left(1 - e^{-\frac{\Lambda_{\text{CCC}}}{C_{\text{CCC}}}} \right)}{(K_{\text{CCC}} - 1) e^{-\frac{\Lambda_{\text{CCC}}}{C_{\text{CCC}}}}} \left(\frac{2d_{\text{сot}} C_{\text{CCC}}}{cD_{\text{mes CCC}}} + \frac{K_{\text{CCC}} - 1}{2} + 1 \right) \right). \quad (5)$$

Пропускная способность ИНС в такой ВКСС будет определяться минимальной эффективной пропускной способностью отдельного звена ИНС:

$$C_{e \text{ ИНС}} = \min\{C_e, C_{e \text{ CCC}}\}, \quad (6)$$

при этом эффективные пропускные способности для отдельных звеньев с учетом выражений (1) и (2) будут определяться как:

1) для СВРС на основе протокола CSMA/CA:

$$C_e = S C, \quad (7)$$

где показатели S , C определяются также как и в выражении (4) для времени задержки передачи пакета.

2) для CCC на основе протокола S-Aloha:

$$C_{e \text{ CCC}} = \frac{\Lambda_{\text{CCC}} (K_{\text{CCC}} - 1) e^{-\frac{\Lambda_{\text{CCC}}}{C_{\text{CCC}}}}}{K_{\text{CCC}} + e^{-\frac{\Lambda_{\text{CCC}}}{C_{\text{CCC}}}}}. \quad (8)$$

Показатели $T_{\text{зад ИНС}}$ (3) и $C_{e \text{ ИНС}}$ (6) формируют показатели качества обслуживания ВКСС с иерархическим принципом информационного обмена.

Модель воздушно-космической сети связи с децентрализованным принципом ретрансляции информационных потоков

Рассмотрим ВКСС с децентрализованным принципом информационного обмена (рис. 5). В данной сети межсетевые ИНС «СВРС-СВРС» могут проходить как через CCC, так и через смежные СВРС объединяемые на основе Mesh-технологий. В предыдущих работах автора получены аналитические соотношения для упрощенного моделирования такой сети. Упрощенная схема вывода основных расчетных соотношений для такой сети представлена на рис. 6. При этом к уже указанным допущениям в данной модели введено

следующее - количество исходящих внешних Mesh-каналов связи из СВРС одинаково и равно z , соответственно связность всех СВРС также одинакова и равна $k_{св}$.

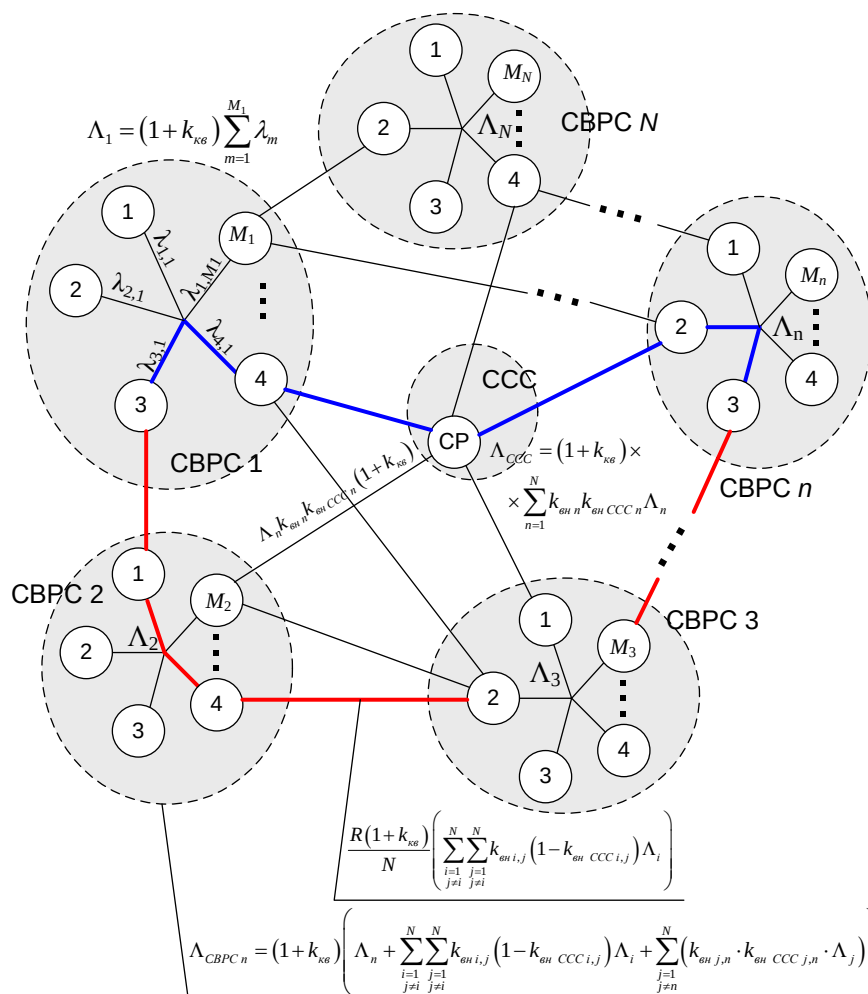


Рис. 5. ВКСС с децентрализованным принципом информационного обмена на основе Mesh-технологий

В соответствии со схемой информационного обмена (рис. 5) и схемой аналитических вычислений для модели ВКСС с децентрализованным принципом информационного обмена (рис. 6) выражения для интенсивности трафика примут вид:

- интенсивность трафика циркулирующего в произвольной СВРС:

$$\Lambda_{CBPC} = \Lambda_1 (1 + k_{kb}) (1 + R k_{вн} (1 - k_{вн CCC}) + k_{вн} \cdot k_{вн CCC}), \quad (9)$$

- интенсивность трафика в CCC:

$$\Lambda_{CCC} = N (1 + k_{kb}) k_{вн} \cdot k_{вн CCC} \cdot \Lambda_1. \quad (10)$$

Общий вид ИНС в децентрализованной ВКСС представлен на рис. 7.

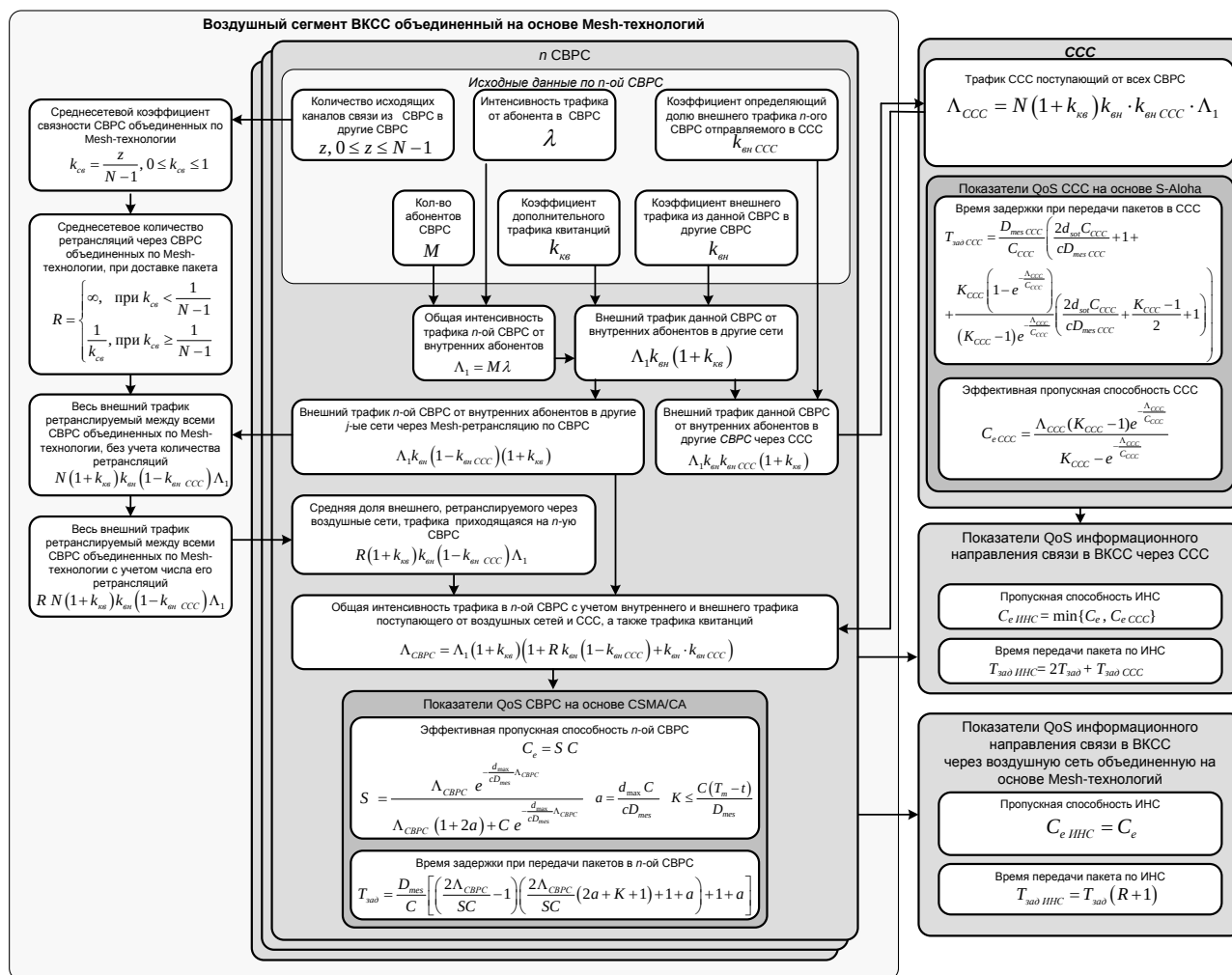


Рис. 6. Упрощенная схема аналитических вычислений для модели ВКС с децентрализованным принципом ретрансляции информационных потоков на основе Mesh-технологий

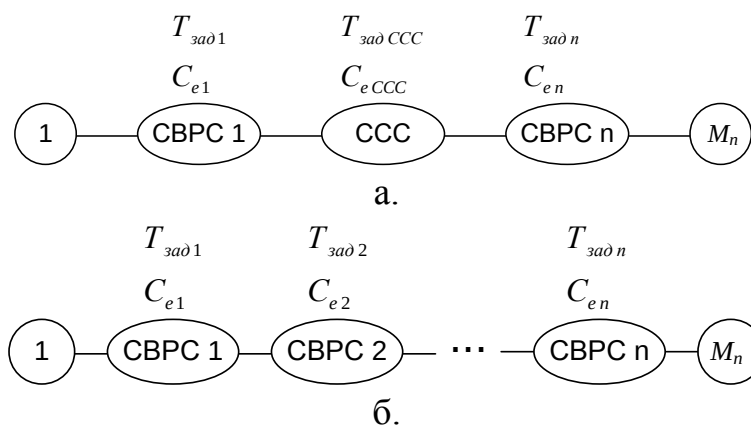


Рис. 7. Общие схемы ИНС в ВКС: а) через CCC; б) ретрансляция через СВРС, соединенных по Mesh-технологии

В ИНС, представленной на рис. 7, время задержки передачи пакета между абонентами разных СВРС будет являться суммой задержек пакета на всех звеньях ИНС:

- при передаче через ССС:

$$T_{\text{зад ИНС}} = 2T_{\text{зад}} + T_{\text{зад ССС}}; \quad (11)$$

- при передаче через СВРС соединенные по Mesh-технологии:

$$T_{\text{зад ИНС}} = T_{\text{зад}}(R+1). \quad (12)$$

При этом время задержки пакета при передаче по отдельным звеньям ИНС будут определяться по выражениям (4) и (5) с учетом выражений для интенсивности трафика $\Lambda_{\text{СВРС}}$ (9) и $\Lambda_{\text{ССС}}$ (10).

Пропускная способность ИНС в такой ВКСС будет определяться минимальной эффективной пропускной способностью отдельного звена ИНС:

- при передаче через ССС:

$$C_{e \text{ ИНС}} = \min\{C_e, C_{e \text{ ССС}}\}; \quad (13)$$

- при передаче через СВРС соединенные по Mesh-технологии:

$$C_{e \text{ ИНС}} = C_e. \quad (14)$$

При этом пропускные способности отдельных звеньев C_e и $C_{e \text{ ССС}}$ в ИНС будут определяться по выражениям (7) и (8) с учетом выражений для интенсивности трафика $\Lambda_{\text{СВРС}}$ (9) и $\Lambda_{\text{ССС}}$ (10).

Анализ качества обслуживания

в воздушно-космической сети связи на основе иерархического принципа ретрансляции информационных потоков

Проведем оценку пропускной способности и времени задержки передачи в ИНС для ВКСС с иерархическим принципом ретрансляции информационных потоков при ограничениях, которые соответствуют техническим характеристикам современных средств связи [1, 7, 8]:

- базовая интенсивность информационного потока в СВРС составляет $\lambda=1,2$ кбит/с;
- количество абонентов СВРС $M=1 \dots 20$, при этом каждый из абонентов генерирует трафик λ ;
- пропускная способность каналов множественного доступа для СВРС равна $C=48$ кбит/с, для ССС - 13,3 кбит/с;
- объемы пакетов в СВРС (D_{mes}) и ССС ($D_{\text{mes ССС}}$) имеют равные значения - 256 бит;
- коэффициенты настойчивости протокола множественного доступа в СВРС и ССС равны и имеют значения $K=K_{\text{ССС}}=16$;
- радиус СВРС равен $d_{\text{max}}=250$ км.

Результаты моделирования представлены на рис. 8-11.

Как показали результаты моделирования, ввиду того, что пропускная способность спутникового сегмента ВКСС существенно ниже пропускной способности СВРС (рис. 8), то общая пропускная способность ИНС в ВКСС определяется пропускной способностью именно ССС сегмента (рис. 10). Такой же вывод можно сделать и о времени задержки передачи сообщений в ИНС (рис. 9, рис. 11) – именно спутниковый сегмент ВКСС определяет задержку передачи по ИНС.

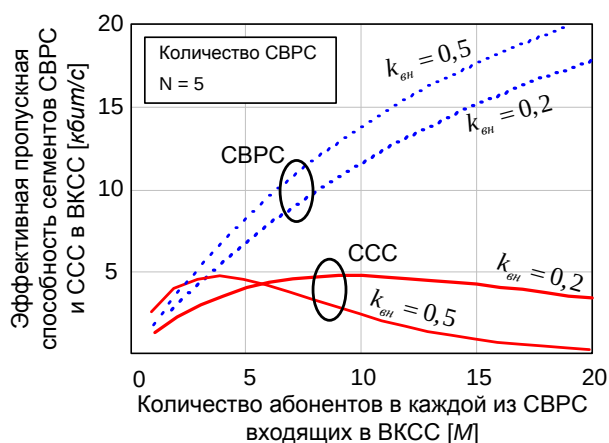


Рис. 8. Пропускная способность спутникового и воздушного сегментов ВКСС с иерархическим принципом информационного обмена

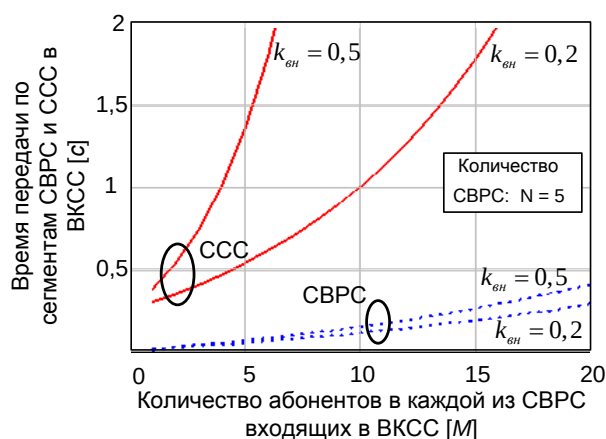
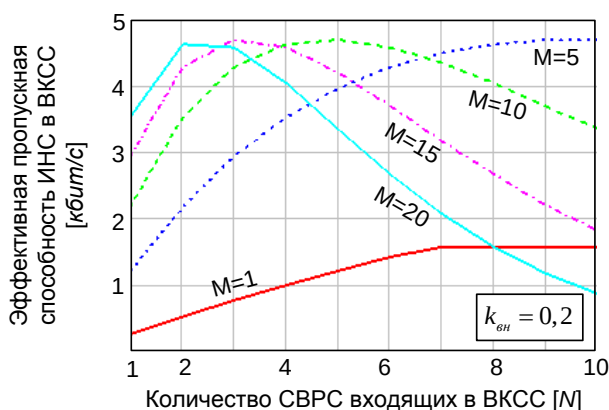
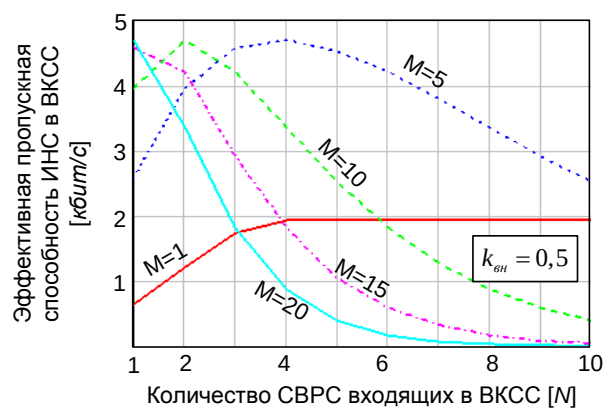


Рис. 9. Время передачи по спутниковому и воздушному сегментам ВКСС с иерархическим принципом информационного обмена

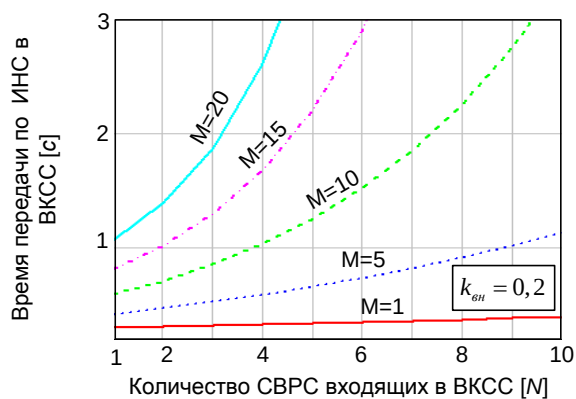


а.

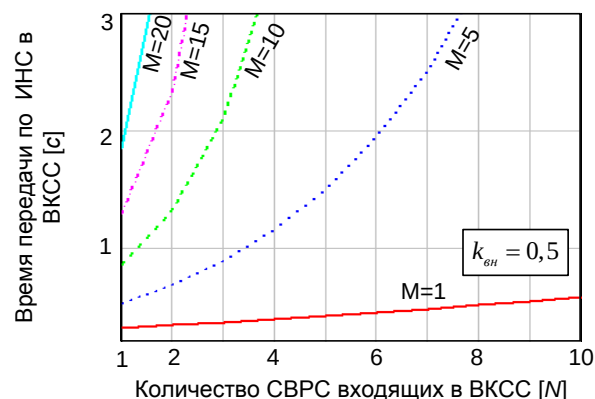


б.

Рис. 10. Пропускная способность ИНС в ВКСС с иерархическим принципом информационного обмена при различных значениях $k_{вн}$



а.



б.

Рис. 11. Время задержки передачи по ИНС в ВКСС с иерархическим принципом информационного обмена при различных значениях $k_{вн}$

Наиболее существенным фактором определяющим QoS ИНС в ВКСС является коэффициент внешнего трафика $k_{вн}$ (рис. 10). По мере роста доли трафика ретранслируемого в другие СВРС нагрузка на ССС увеличивается. С учетом того, что именно ССС является звеном в ИНС с наименьшей

пропускной способностью, это приводит к резкому увеличению времени передачи сообщений по ИНС в ВКС (рис. 11). В результате значения ВКС не позволяет обслужить мультимедийный трафик (речь, видео, изображения, передаваемые в реальном времени), так как требуемое время задержки, при его передачи не должно превышать 0,5-0,6 с.

Фактически предельные возможности по структуре ВКС для передачи трафика реального времени ($T_m < 0,6$ с) – 4 СВРС в каждой не более 5 абонентов по 1,2 кбит/с, при коэффициенте внешнего трафика $k_{\text{вн}} \leq 0,2$.

Рассмотрим возможности ВКС по обслуживанию мультимедийного трафика (речь, видео, изображения, передаваемые в реальном времени) с учетом перспектив развития авиационных систем связи и планируемого увеличения пропускных способностей канала ССС до 2 Мбит/с, а СВРС – до 34 Мбит/с. С учетом того, что минимальный требуемый канал для передачи мультимедийного трафика составит 16 кбит/с.

Проведем моделирование возможностей перспективной ВКС при ограничениях, которые соответствуют техническим характеристикам перспективных средств связи:

- базовая интенсивность информационного потока в СВРС составляет $\lambda = 16$ кбит/с;
- количество абонентов СВРС $M = 1 \dots 20$, при этом каждый из абонентов генерирует трафик λ ;
- пропускная способность каналов множественного доступа для СВРС равна $C = 34$ Мбит/с, для ССС – 2 Мбит/с;
- объемы пакетов в СВРС (D_{mes}) и ССС ($D_{\text{mes ССС}}$) имеют равные значения – 256 бит;
- коэффициенты настойчивости протокола множественного доступа в СВРС и ССС равны и имеют значения $K = K_{\text{ССС}} = 16$;
- радиус СВРС равен $d_{\text{max}} = 250$ км.

Результаты моделирования представлены на рис. 12-15.

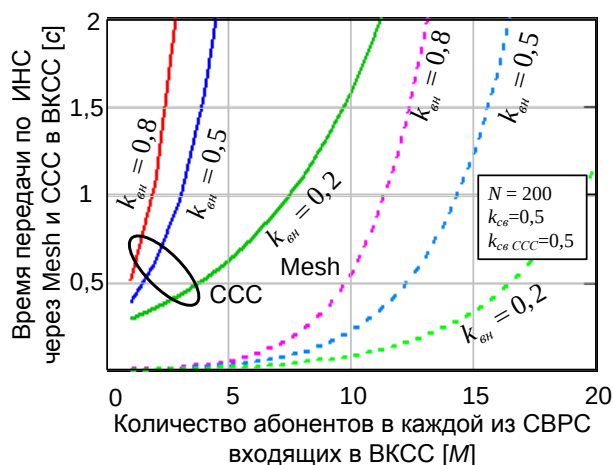


Рис. 12. Пропускная способность спутникового и воздушного сегментов ВКС с иерархическим принципом информационного обмена

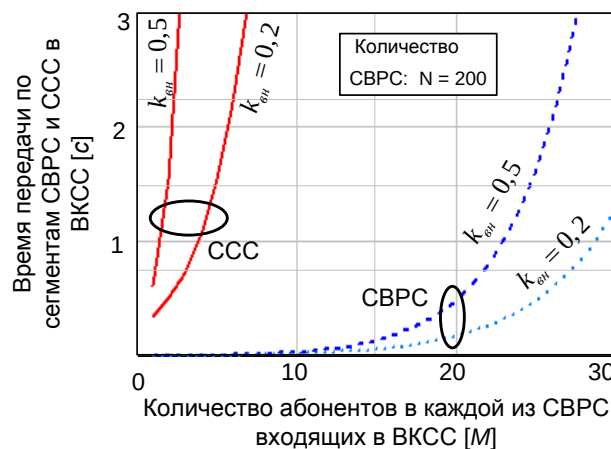


Рис. 13. Время передачи по спутниковому и воздушному сегментам ВКС с иерархическим принципом информационного обмена

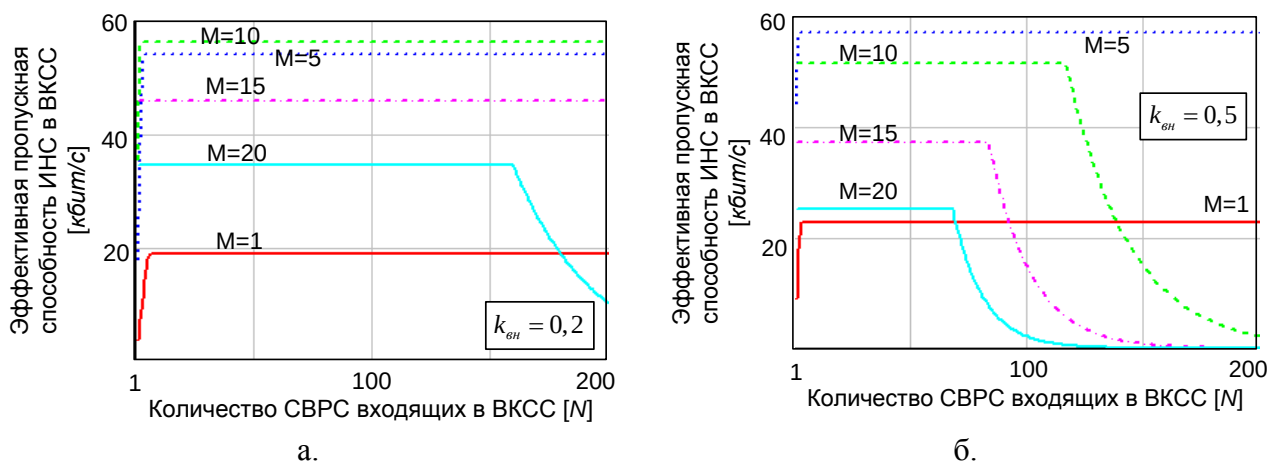


Рис. 14. Пропускная способность ИНС в ВКСС с иерархическим принципом информационного обмена при различных значениях $k_{вн}$

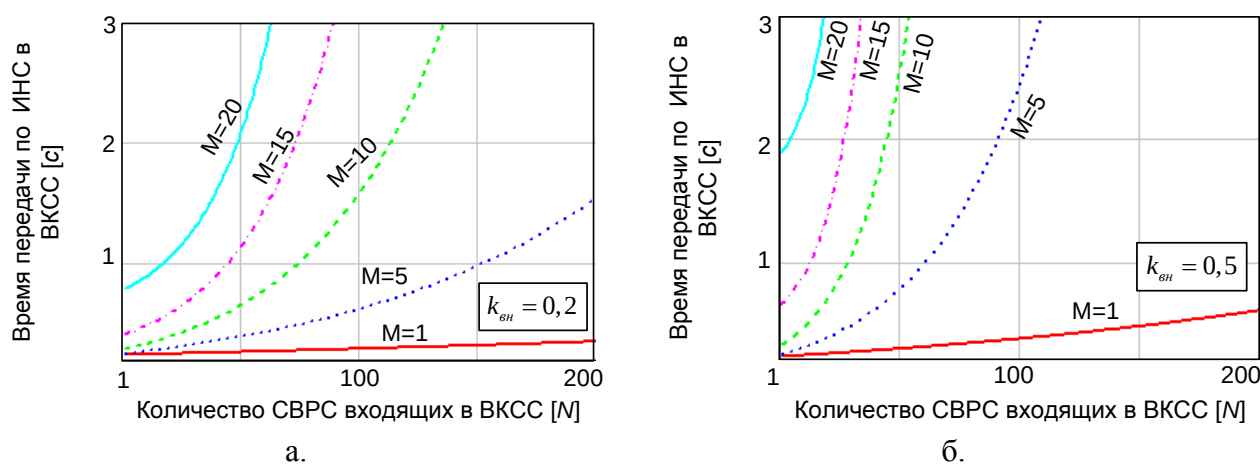


Рис. 15. Время задержки передачи по ИНС в ВКСС с иерархическим принципом информационного обмена при различных значениях $k_{вн}$

Анализ графиков на рис. 12-15 показывают, что факторы более низкой пропускной способности ССС и зависимость QoS ИНС от коэффициента внешнего трафика $k_{вн}$ продолжают играть свою роль. Как видно на рис. 14 именно снижение пропускной способности ССС ведет к снижению пропускной способности ИНС после достижения критических значений соотношения абонентов M и числа СВРС N .

Анализ графиков на рис. 15 позволяет определить предельные возможности по структуре перспективной ВКСС для передачи трафика реального времени ($T_m < 0,6$ с):

- при коэффициенте внешнего трафика до $k_{вн} \leq 0,2$:
 - а) до 100 СВРС в каждой не более 5 абонентов по 16 кбит/с;
 - б) до 50 СВРС в каждой не более 10 абонентов по 16 кбит/с;
 - в) до 30 СВРС в каждой не более 15 абонентов по 16 кбит/с;
- при коэффициенте внешнего трафика до $k_{вн} \leq 0,5$:
 - а) до 40 СВРС в каждой не более 5 абонентов по 16 кбит/с;
 - б) до 17 СВРС в каждой не более 10 абонентов по 16 кбит/с;
 - в) до 2 СВРС в каждой не более 15 абонентов по 16 кбит/с.

Сравнительный анализ качества обслуживания в воздушно-космической сети связи на основе иерархического и децентрализованного принципа ретрансляции информационных потоков

Проведем оценку пропускной способности и времени задержки передачи в ИНС для ВКСС с децентрализованным принципом ретрансляции информационных потоков. При ограничениях, которые соответствуют техническим характеристикам современных средств связи [1, 7, 8]:

- базовая интенсивность информационного потока в СВРС составляет $\lambda=1,2$ кбит/с;
- количество абонентов СВРС $M=1 \dots 20$, при этом каждый из абонентов генерирует трафик λ ;
- пропускная способность каналов множественного доступа для СВРС равна $C=48$ кбит/с, для CCC - 13,3 кбит/с;
- объемы пакетов в СВРС (D_{mes}) и CCC ($D_{mes\ CCC}$) имеют равные значения - 256 бит;
- коэффициенты настойчивости протокола множественного доступа в СВРС и CCC равны и имеют значения $K=K_{CCC}=16$;
- радиус СВРС равен $d_{max}=250$ км.

Результаты моделирования представлены на рис. 16-19.

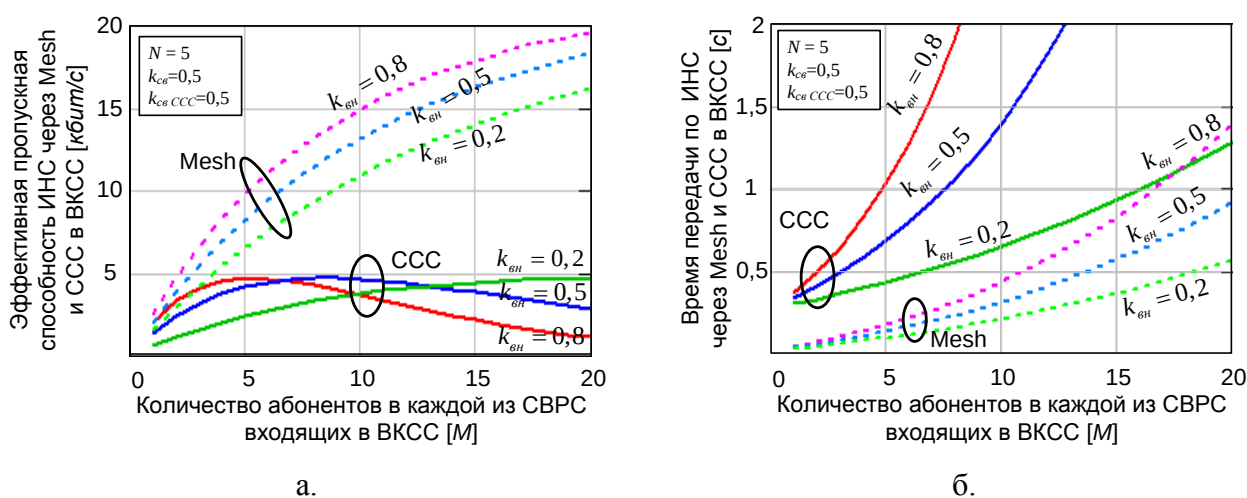


Рис. 16. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКСС с децентрализованным принципом информационного обмена при различных значениях количества абонентов M

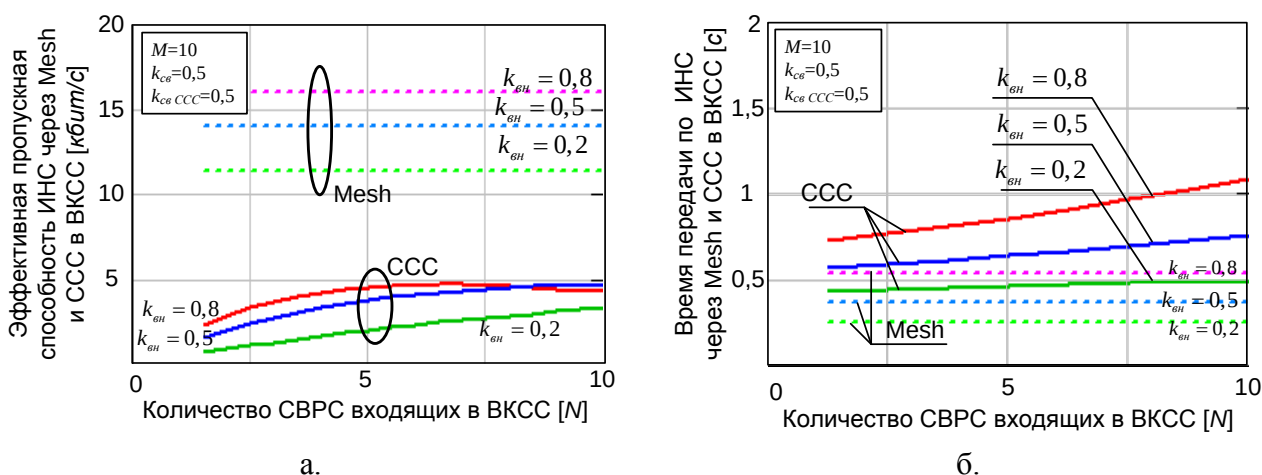


Рис. 17. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом информационного обмена при различных значениях количества сетей N

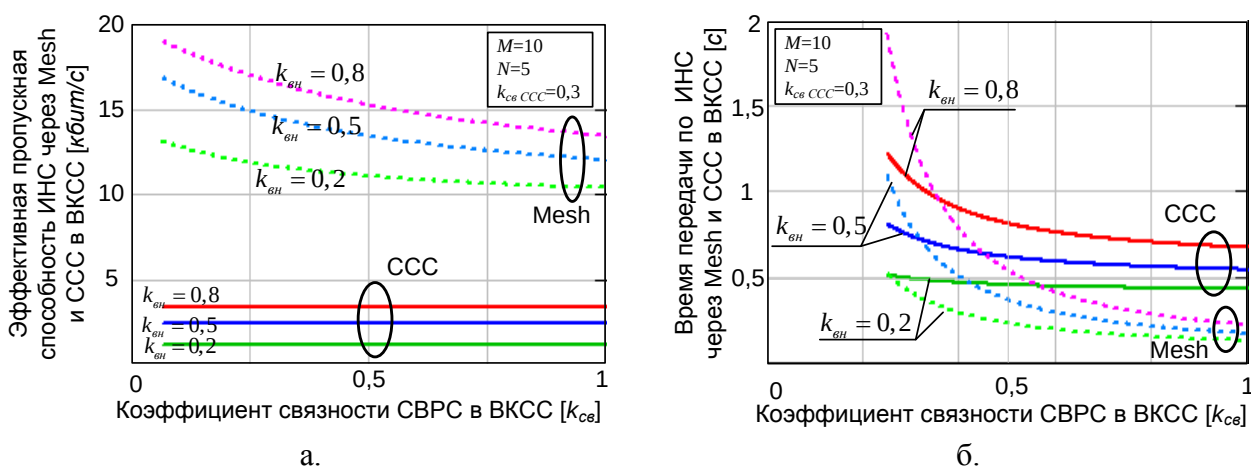


Рис. 18. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом информационного обмена при изменении связности СВРС

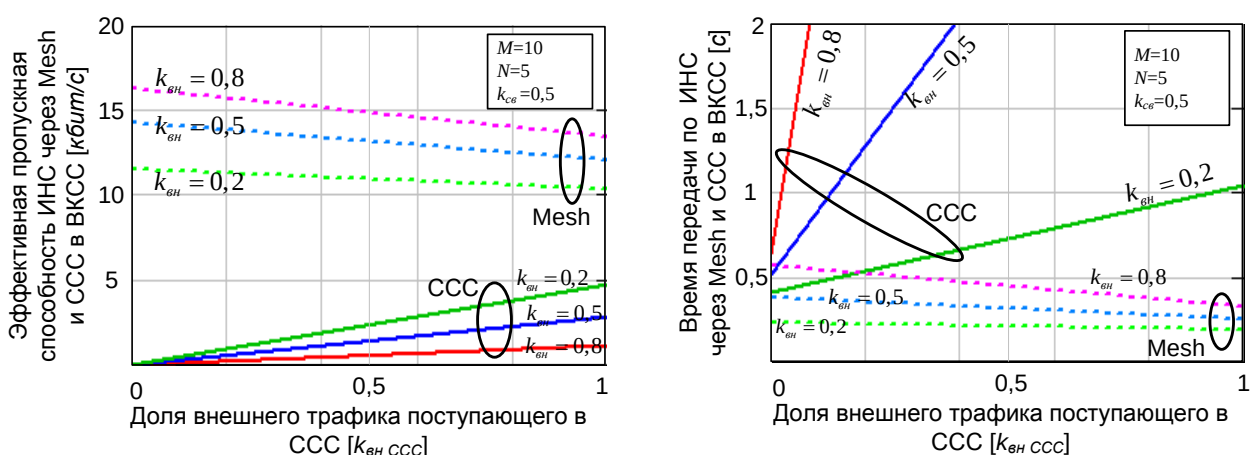


Рис. 19. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом информационного обмена при изменении доли трафика в составе внешнего трафика поступающего в CCC

Анализ графических зависимостей на рис. 16-19 показывают, что в целом наиболее существенным фактором определяющим QoS ИНС в ВКСС продолжает оставаться коэффициент внешнего трафика $k_{вн}$. Однако использование Mesh-технологии объединений СВРС позволяет ретранслировать часть трафика в смежные СВРС (определяется коэффициентом $k_{вн\ CCC}$), тем самым существенно разгрузить спутниковый сегмент ВКСС и как следствие снизить время передачи сообщений по ИНС. При этом эффективность применения Mesh-технологий полностью определяется коэффициентом связности воздушных сетей $k_{св}$. Таким образом, внедрение Mesh-технологии без изменения технических характеристик оборудования по пропускной способности не позволяют существенно изменить ситуацию с невозможность построения глобальных сетей ретрансляции трафика реального времени.

Предельные возможности по структуре ВКСС для передачи мультимедийного трафика ($T_m < 0,6$ с), при коэффициенте связности воздушного сегмента $k_{св} \geq 0,5$:

- до 10 СВРС в каждой не более 10 абонентов по 1,2 кбит/с:
 - а) при коэффициентах внешнего трафика $k_{вн} \leq 0,5$, $k_{вн\ CCC} = 0$;
 - б) при коэффициентах внешнего трафика $k_{вн} \leq 0,2$, $k_{вн\ CCC} \leq 0,05$;
- до 5 СВРС в каждой не более 12 абонентов по 1,2 кбит/с:
 - а) при коэффициентах внешнего трафика $k_{вн} \leq 0,5$, $k_{вн\ CCC} = 0$;
 - б) при коэффициентах внешнего трафика $k_{вн} \leq 0,2$, $k_{вн\ CCC} \leq 0,05$.

Таким образом, с одной стороны использование Mesh-технологии позволяет увеличить емкость ВКСС и ее возможности по обслуживанию трафика реального времени, а с другой стороны, возникает множество вариантов балансировки трафика между воздушным и спутниковым сегментами ССС, что требует разработки отдельной методики балансировки нагрузки.

Рассмотрим возможности ВКСС по обслуживанию мультимедийного трафика с учетом планируемого увеличения пропускных способностей канала ССС до 2 Мбит/с, а СВРС – до 34 Мбит/с. С учетом того, что минимальный требуемый канал для передачи мультимедийного трафика составит 16 кбит/с.

Проведем моделирование возможностей перспективной ВКСС при ограничениях, которые соответствуют техническим характеристикам перспективных средств связи:

- базовая интенсивность информационного потока в СВРС составляет $\lambda = 16$ кбит/с;
- количество абонентов СВРС $M = 1 \dots 20$, при этом каждый из абонентов генерирует трафик λ ;
- пропускная способность каналов множественного доступа для СВРС равна $C = 34$ Мбит/с, для ССС - 2 Мбит/с;
- объемы пакетов в СВРС (D_{mes}) и ССС ($D_{mes\ CCC}$) имеют равные значения - 256 бит;
- коэффициенты настойчивости протокола множественного доступа в СВРС и ССС равны и имеют значения $K = K_{CCC} = 16$;

- радиус СВРС равен $d_{\max}=250$ км.

Результаты моделирования представлены на рис. 20-23.

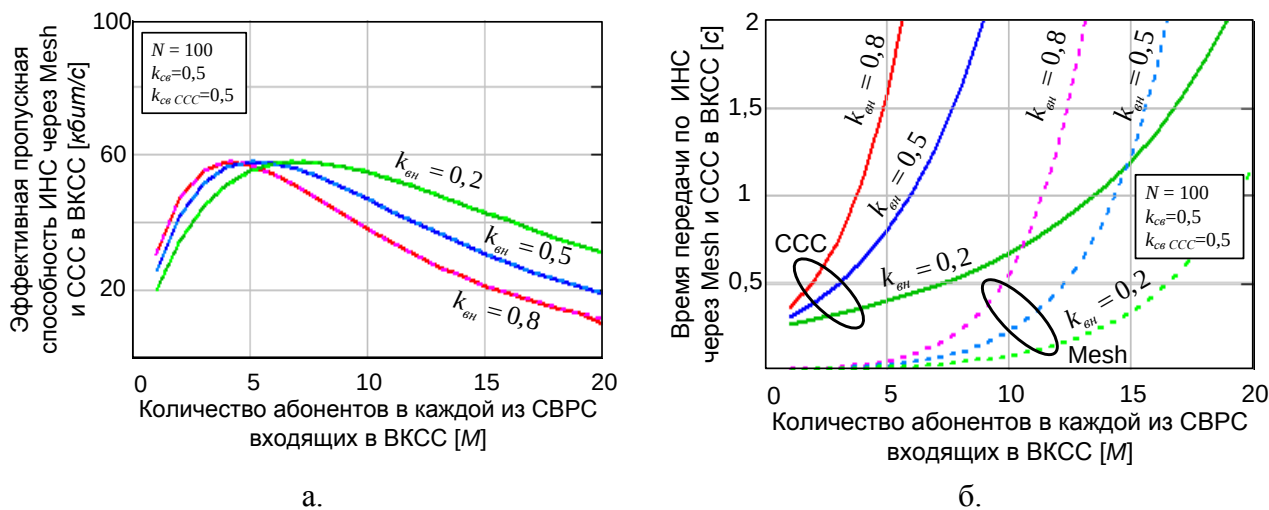


Рис. 20. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом информационного обмена при различных значениях количества абонентов M

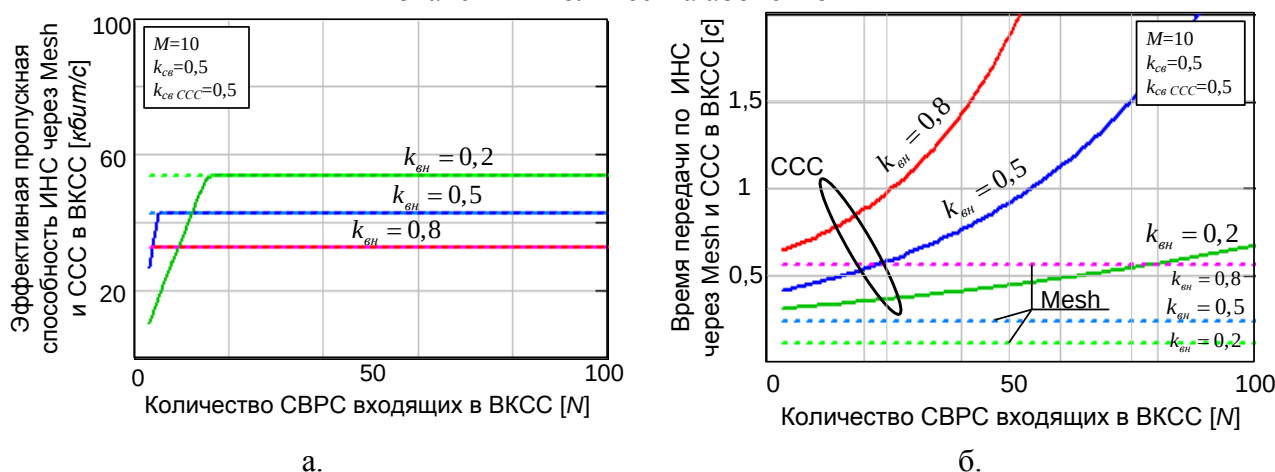


Рис. 21. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом информационного обмена при различных значениях количества сетей N

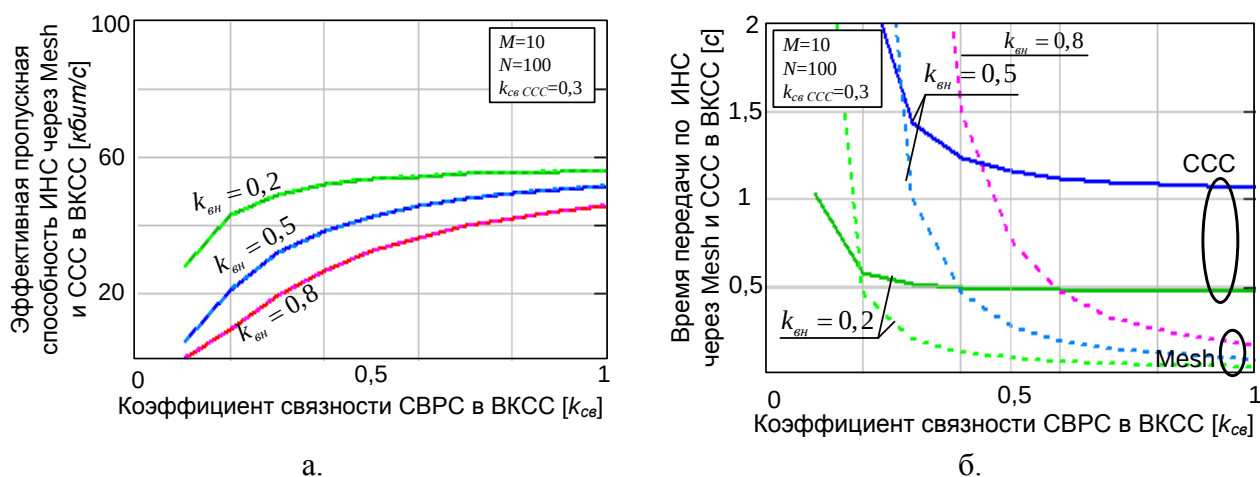


Рис. 22. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом передачи при изменении связности СВРС

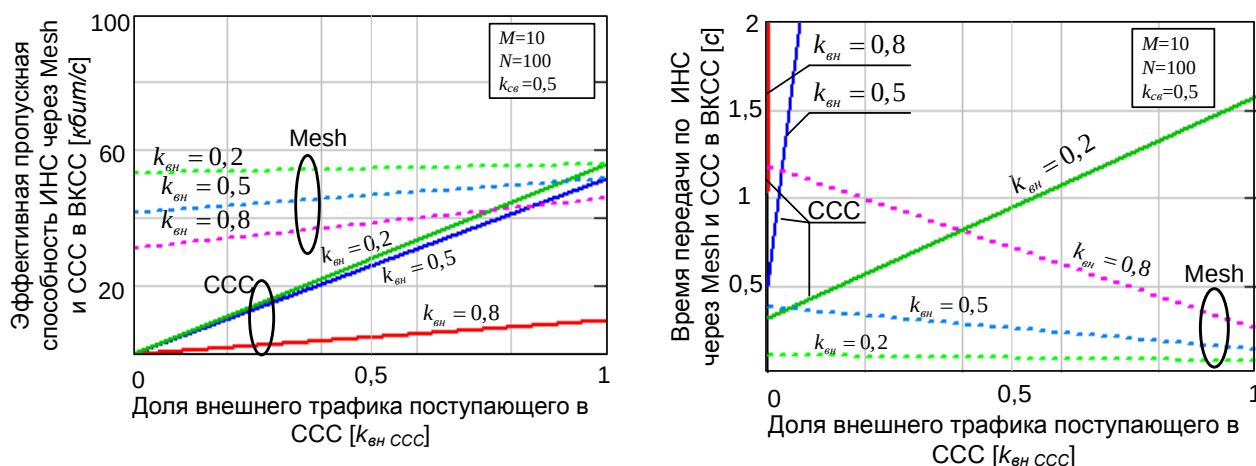


Рис. 23. Пропускная способность и время передачи по ИНС (через CCC и через Mesh) в ВКС с децентрализованным принципом информационного обмена при изменении доли трафика в составе внешнего трафика поступающего в CCC

Анализ графиков на рис. 20-23 показывает, что в ВКС построенном на основе децентрализованного принципа информационного обмена в зависимости от коэффициентов $k_{вн}$ и $k_{вн\ CCC}$ звеном с наиболее низкой пропускной способностью может выступать как CCC так и воздушный сегмент ВКС (рис. 21а). При этом соотношение коэффициентов $k_{вн}$ и $k_{вн\ CCC}$ фактически определяют поведение всей системы.

Графические зависимости на рис. 20-23 позволяет определить предельные возможности по структуре перспективной ВКС для передачи трафика реального времени ($T_m < 0,6$ с):

- при коэффициенте внешнего трафика до $k_{вн} \leq 0,2$ ($k_{вн\ CCC} \leq 0,15$, $k_{cg} = 0,5$):
 - а) до 100 СВРС в каждой не более 10 абонентов по 16 кбит/с;
 - б) до 70 СВРС в каждой не более 10 абонентов по 16 кбит/с;
- при коэффициенте внешнего трафика до $k_{вн} \leq 0,6$ ($k_{вн\ CCC} = 0$, $k_{cg} = 0,5$):
 - а) до 200 СВРС в каждой не более 10 абонентов по 16 кбит/с.

Представим итоговые данные о повышении пропускной способности по показателю общего количества обслуживаемых абонентов за счет использования Mesh-технологий в ВКС в виде таблицы 6.

Анализ результатов представленных в таблице позволяет сделать вывод о том, что использование Mesh-технологий для объединения СВРС в воздушном сегменте, позволяет ретранслировать большую часть трафика ВКС через смежные СВРС и тем самым повысить пропускную способности ВКС по показателю одновременного числа обслуживаемых абонентов в 2...4 раза, для современного авиационного оборудования связи и до 9 раз – для перспективного.

Таблица 6. Повышение пропускной способности

Параметры информационных потоков		ВКСС (ССС)	ВКСС (ССС+Mesh, $k_{св}=0,5$)	Прирост пропускной способности (в аб.)
Современное оборудование авиационной связи				
$\lambda=1,2$ кбит/с	$k_{вн} \leq 0,2$	4×5 аб.	10×10 аб.	до 400%
			5×12 аб.	до 200%
	$k_{вн} \leq 0,5$	-	10×10 аб.	∞
		-	5×12 аб.	∞
Перспективное оборудование авиационной связи				
$\lambda=16$ кбит/с	$k_{вн} \leq 0,2$	100×5 аб. 50×10 аб.	200×10 аб.	до 300%
	$k_{вн} \leq 0,5$	40×5 аб. 17×10 аб.	200×10 аб.	до 900%

Выводы

Таким образом, использование Mesh технологии позволяет в разы повысить пропускную способность ВКСС по количеству одновременно обслуживаемых абонентов, передающих мультимедийный трафик. Однако, такое повышение реализуется за счет использования избыточного ресурса пропускной способности СВРС и фактически ведет к ретрансляции подавляющей части трафика ВКСС через воздушный сегмент. При этом, доли ретранслируемого трафика определяется параметрами $k_{вн}$ и $k_{вн\ СССР}$, а время задержки еще и зависит от коэффициента связности $k_{св}$ который напрямую определяет количество шагов ретрансляции.

Представленная схема построения ВКСС в интересах информационного обеспечения авиации является развитием работ [14, 15, 18-23] по созданию многоуровневых и гибридных систем связи передачи мультимедийного трафика на основе СССР. Предложения по использованию Mesh технологии в интересах повышения пропускной способности ВКСС развивают актуальное направление исследований представленное в работах [5-6, 24-32] и посвященные увеличению пропускной способности сетей авиационной связи за счет использования современных информационных технологий.

Ввиду того, что прирост пропускной способности ВКСС обеспечивается при различных соотношениях трафика направляемого в воздушный и космический сегменты дальнейшие исследования целесообразно направить на разработку методики балансировки информационных потоков в ВКСС, по аналогии с работой [33]. Целью этой методики должно стать обоснование рационального значения параметра $k_{вн\ СССР}$ при заданных параметрах ВКСС $k_{вн}$, $k_{св}$, M , N , с целью максимизировать пропускную способность ВКСС. Решение этой задачи, планируется в последующих работах автора.

Литература

1. Авиация ПВО России и научно технический прогресс: боевые комплексы и системы вчера, сегодня, завтра: монография / под ред. Федосова Е.А. – М.: Дрофа, 2005. – 815 с.

2. Связь в Вооруженных силах Российской Федерации – 2013: тематический сборник. / Под ред. Абрамовича А.В., Герасимова А.В., Цибина С.В., Ометова К.С., Быстрова Ю.А. М.: ООО «Компания «Информационный мост», 2013. 216 с. URL: www.informost.ru (дата доступа 01.08.2015).
3. Оружие и технологии России. Энциклопедия. XXI век. Системы управления, связи и радиоэлектронной борьбы / Под общ. ред. Иванова С. М.: Изд. дом «Оружие и технологии», 2006. 695 с.
4. Легков К. Е. Методы повышения производительности беспроводных mesh-сетей специального назначения // Т-Comm. 2011. № 3. С. 46-48.
5. Кулаков М. С. Анализ особенностей функционирования мобильных самоорганизующихся сетей MANET на уровне доступа к среде MAC // Т-Comm. 2014. № 10. С. 39-42.
6. Кулаков М. С. Применение алгоритмов самоорганизации для режима VDL-2 // Фундаментальные проблемы радиоэлектронного приборостроения. 2012. Т. 5. № 5. С. 58-62.
7. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.
8. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: – Свое издательство, 2013. – 166 с.
9. Макаренко С. И., Рюмшин К. Ю., Михайлов Р. Л. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147.
10. Макаренко С. И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2-2. - URL: <http://jre.cplire.ru/jre/sep11/4/text.pdf> (дата доступа 03.08.2015).
11. Макаренко С. И. Оценка качества обслуживания пакетной радиосети в нестационарном режиме в условиях воздействия внешних дестабилизирующих факторов // Журнал радиоэлектроники. 2012. № 6. – URL: <http://jre.cplire.ru/jre/jun12/9/text.pdf> (дата доступа 03.02.2015).
12. Макаренко С. И., Михайлов Р. Л., Новиков Е. А. Исследование канальных и сетевых параметров канала связи в условиях динамически изменяющейся сигнально–помеховой обстановки // Журнал радиоэлектроники. 2014. № 10. - URL: <http://jre.cplire.ru/jre/oct14/3/text.pdf> (дата доступа 03.08.2015).
13. Научно-производственное предприятие «Полет». Официальный сайт. [Электронный ресурс]. 2015. URL: <http://www.polyot.atnn.ru> (дата доступа 03.08.2015).
14. Телегин Г. А., Моисеев Н. И., Демидов А. С., Рязанцев О. Д., Алыбин В. Г. Спутниковые интегрированные телекоммуникационные сети на

технологии ATM // 11 Международная конференция «Микроволновые и телекоммуникационные технологии» (CriMiCo'2001). 10-14 сентября. Севастополь, 2001.

15. Кузенков А. В. Состояние и перспективы развития отечественных ретрансляторов // Аэрокосмический курьер. 2013. № 2. С. 42-45.

16. Назаров А. Н., Сычев К. И. Модели и методы расчёта показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. - Красноярск: изд. ООО "Поликом", 2010.— 389 с.

17. Макаренко С. И., Бородинов Р. В. Анализ технологий обеспечения качества обслуживания в мультисервисных ATM сетях // Информационные технологии моделирования и управления. 2012. №1 (73). С. 65-79.

18. Пастухов А. С., Перегняк А. Е., Лукьянцев С. А., Симонян А. Г. Оценка взаимного влияния самоподобных Internet- и видеотрафика при передаче по гибридным сетям спутниковой связи // Электротехнические и информационные процессы. 2009. Т. 5. № 1. С. 58-61.

19. Пастухов А. С., Разумов Я. М., Окулов К. Ю., Гуреев А. К. Моделирование совместной передачи видео- и Internet-трафика в стандарте DVB/IP/MPEG-2 в гибридных спутниковых сетях связи // Электротехнические и информационные процессы. 2007. Т. 3. № 2. С. 56-60.

20. Мальцев Г. Н., Цветков К. Ю., Родионов А. В., Акмоллов А. Ф., Ефимов С. Н., Косаревиц Д. В., Викторов Е. А. Концепция построения разнорысотной многоспутниковой системы связи с мобильными абонентами // Труды Военно-космической академии имени А.Ф. Можайского. 2011. № 630. С. 5-10.

21. Chen. C., Ekici E. A Routing Protocol for Hierarchical LEO/MEO Satellite IP Networks // Wireless Networks. 2005. no. 11. pp. 507–521.

22. Durresi A., Dash D., Anderson B.L., Kannan R., Kota S., Jain R. Routing of Real-time Traffic in a Transformational Communications Architecture // Aerospace Conference, IEEE. 2004. Vol. 2. pp. 1086-1104.

23. Akyildiz I. F., Ekici E., Bender M. D. MLSP: A Novel Routing Algorithm for Multilayered Satellite IP Networks // IEEE/ACM transactions on networking. Vol. 10. No. 3. 2002. pp. 411-424.

24. Алехин С. В., Войткевич К. Л. Моделирование протокола маршрутизации для беспроводных мобильных сетей // Электросвязь. 2014. № 7. С. 7-8.

25. Войткевич К. Л., Сулима А. А., Зац П. А. Проблемы построения канала управления беспилотными летательными аппаратами на основе ДКМВ-радиолонии // Электросвязь. 2014. № 7. С. 9-11.

26. Войткевич К. Л., Резвов А. В., Шанин В. Н. Специализированные локальные беспроводные мобильные сети гражданского и военного назначения // Системы и средства связи, телевидения и радиовещания. 2013. № 1-2. С. 130-133.

27. Комяков А. В., Войткевич К. Л., Сулима А. А. Инновационные решения для перспективных летательных аппаратов // Деловая слава России. 2013. № 3 (41). С. 26-27.
28. Белоусов Е. Л., Брянцев В. Ф., Войткевич К. Л., Кейстович А. В., Сайфетдинов Х. И. Вопросы создания авиационного радиосвязного оборудования по принципу «программируемое радио» // Труды НГТУ им. Р.Е. Алексеева. 2012. № 2 (95). С. 11-18.
29. Белоусов Е. Л., Брянцев В. Ф., Войткевич К. Л., Кейстович А. В., Сайфетдинов Х. И. Перспективное бортовое оборудование сети авиационной радиосвязи // Труды НГТУ им. Р.Е. Алексеева. 2012. № 3 (96). С. 11.
30. Войткевич К. Л. Опыт по созданию бортовых комплексов связи для самолетов тактического звена управления // Системы и средства связи, телевидения и радиовещания. 2009. № 1-2. С. 42-43.
31. Макаренко С. И. Адаптивное управление скоростями логических соединений в канале радиосвязи множественного доступа // Информационно-управляющие системы. 2008. № 6. С. 54-58.
32. Прохоров А. В., Бондарь Д. С. Применение аппаратуры широкополосного радиодоступа в локальных сетях связи и передачи данных систем управления воздушным движением // Научный вестник Московского государственного технического университета гражданской авиации. 2012. № 176. С. 93-100.
33. Иванов В. И. Централизованный метод балансировки нагрузки в низкоорбитальной спутниковой системе // T-Comm. 2014. № 4. С. 38-42.

References

1. Fedosov E. A. *Aviatsiia PVO Rossii i nauchno tekhnicheskii progress: boevye komplekсы i sistemy vchera, segodnia, zavtra. Monografiia* [Air Defence of Russia and Scientific Technical Progress: Combat Systems and Systems Yesterday, Today, Tomorrow. Treatise]. Moscow, Drofav Publ., 2005, 815 p. (in Russian).
2. Abramovich A. V., Gerasimov A. V., Tsibin S. V., Ometov K. S., Bystrov Iu. A. *Sviaz' v Vooruzhennykh silakh Rossiiskoi Federatsii - 2013: tematicheskii sbornik* [Communication in the Armed Forces of the Russian Federation - 2013: Thematic Collection]. Moscow, "Company "Information Bridge" Publ., 2013, 216 p. Available at: www.informost.ru (accessed 03 February 2015) (in Russian).
3. Ivanov S. *Oruzhie i tekhnologii Rossii. Entsiklopediia. XXI vek. Sistemy upravleniia, sviazi i radioelektronnoi bor'by* [Weapons and Technology of Russia. The Encyclopedia. XXI Century. Control Systems, Communications and Electronic Warfare]. Moscow, "Weapons and Technology" Publ., 2006, 695 p. (In Russian).
4. Legkov K. E. Methods of increase of productivity of wireless mesh-networks of a special purpose. *T-Comm*, 2011, no. 3, pp. 46-48 (in Russian).
5. Kulakov M. S. Analysis of functioning of mobile self_organizing networks MANET on the media access control layer MAC. *T-Comm*, 2014, no. 10, pp. 39-42 (in Russian).

6. Kulakov M. S. Primenenie algoritmov samoorganizatsii dlia rezhima VDL-2 [The application of self-organization algorithms for VDL-2 mode]. *Fundamental'nye problemy radioelektronnogo priborostroeniia*, 2012, vol. 5, no. 5, pp. 58-62 (in Russian).
7. Antonovich P. I., Makarenko S. I., Mihaylov R. L., Ushanev K. V. New means of destructive effects on network centric military command, control and communication systems in the information space. *Vestnik Akademii voennykh nauk*, 2014, vol. 48, no. 3, pp. 93-101 (in Russian).
8. Makarenko S. I., Ivanov M. S., Popov S. A. *Pomekhozashchishchennost' sistem sviazi s psevdosluchainoi perestroikoi rabochei chastoty. Monografiia* [Interference Resistance Communication Systems with Frequency-Hopping Spread Spectrum. Treatise]. St-Petersburg, Svoe Izdatel'stvo Publ., 2013, 166 p. (in Russian).
9. Makarenko S. I., Ryimshin K. Yu., Mikhailov R. L. Model' funktsionirovaniia ob"ekta seti sviazi v usloviiakh ogranichennoi nadezhnosti kanalov sviazi [Model of Functioning of Telecommunication Object in the Limited Reliability of Communication Channel Conditions]. *Information Systems and Technologies*, 2014, no. 6, pp. 139-147 (in Russian).
10. Makarenko S. I. The Countermeasures of the Radio Networks with the Random Multiple Access by Changing the Radionet State to Non-Stable. *Radio electronics journal*, 2011, no. 9. Available at: <http://jre.cplire.ru/jre/sep11/4/text.pdf> (accessed 01 August 2015) (in Russian).
11. Makarenko S. I. Estimation of quality of service in radio network with package transmitting in unstationary mode under influence of external destructive factors. *Radio Electronics Journal*, 2012, no. 6. Available at: <http://jre.cplire.ru/jre/jun12/9/text.pdf> (accessed 01 August 2015) (in Russian).
12. Makarenko S. I., Mikhailov R. L., Novikov E. A. Issledovanie kanal'nykh i setevykh parametrov kanala sviazi v usloviiakh dinamicheskii izmeniaiushcheisia signal'no-pomekhovoi obstanovki [The Research of Data Link Layer and Network Layer Parameters of Communication Channel in the Conditions Dynamic Vary of the Signal and Noise Situation]. *Journal of Radio Electronics*, 2014, no. 10. Available at: <http://jre.cplire.ru/jre/oct14/3/text.pdf> (accessed 01 August 2015) (in Russian).
13. Nauchno-proizvodstvennoe predpriatie "Polet". Available at: <http://www.polyot.atnn.ru> (accessed 03 February 2015) (in Russia).
14. Telegin G. A., Moiseev N. I., Demidov A. S., Ryazantsev O. D., Alybin V. G. Sputnikovye integrirovannye telekommunikatsionnye seti na tekhnologii ATM [Satellite Integrated Telecommunication Networks Based on ATM-Technology]. *11-th International Conference "Microwave & Telecommunication Technology" (CriMiCo'2001), 10-14 September, Sevastopol, 2001*.
15. Kuzenkov A. Sostoianie i perspektivy razvitiia otechestvennykh retransliatorov [The State and Prospects of Development of Domestic Repeaters]. *Aerospace courier*, 2013, vol. 2, pp. 42-45 (in Russian).

16. Nazarov A. N., Sychev K. I. *Modeli i metody rascheta pokazatelei kachestva funktsionirovaniia uzlovogo oborudovaniia i strukturno-setevykh parametrov setei sviazi sleduiushchego pokoleniia* [Models and methods of calculation of quality performance of the nodal equipment and structural network parameters of the networks to the next generation]. Krasnoyarsk, Polikom Publ., 2010, 389 p. (in Russian).
17. Makarenko S. I., Borodinov R. V. *Analiz tekhnologii obespecheniia kachestva obsluzhivaniia v mul'tiservisnykh ATM setiakh* [The Analysis of Technologies to Ensure Quality of Service in Multiservice ATM Networks], *Informatsionnye tekhnologii modelirovaniia i upravleniia*, 2012, vol. 73, no. 1, pp. 65-79. (in Russian).
18. Pastukhov A. S., Peregniak A. E., Luk'iantsev S. A., Simonian A. G. *Otsenka vzaimnogo vliianiia samopodobnykh Internet - i videotrafika pri peredache po gibridnym setiam sputnikovoi sviazi* [Assessment of Interference of Self-Similar Internet and Video Traffic During Transmission Over Hybrid Networks Satellite Networks]. *Elektrotekhnicheskie i informatsionnye komplekсы i sistemy*, 2009, vol. 5, № 1, pp. 58-61 (in Russian).
19. Pastukhov A. S., Razumov Ia. M., Okulov K. Iu., Gureev A. K. *Modelirovanie sovmestnoi peredachi video- i Internet-trafika v standarte DVB/IP/MPEG-2 v gibridnykh sputnikovykh setiakh sviazi* [Modeling joint video and Internet traffic as standard DVB/IP/MPEG-2 in hybrid satellite networks]. *Elektrotekhnicheskie i informatsionnye komplekсы i sistemy*, 2007, vol. 3, no. 2, pp. 56-60 (in Russian).
20. Mal'tsev G. N., Tsvetkov K. Iu., Rodionov A. V., Akmolov A. F., Efimov S. N., Kosarevich D. V., Viktorov E. A. The concept of building different multi-satellite communications system with mobile subscribers. *Trudy Voenno-Kosmicheskoi Akademii Imeni A. F. Mozhaiskogo*, 2011, no. 630, pp. 5-10 (in Russian).
21. Chen. C., Ekici E. A Routing Protocol for Hierarchical LEO/MEO Satellite IP Networks. *Wireless Networks*, 2005, no. 11, pp. 507–521.
22. Durresi A., Dash D., Anderson B. L., Kannan R., Kota S., Jain R. Routing of Real-time Traffic in a Transformational Communications Architecture. *Aerospace Conference*, IEEE, 2004, vol. 2, pp. 1086-1104.
23. Akyildiz I. F., Ekici E., Bender M. D. MLSR: A Novel Routing Algorithm for Multilayered Satellite IP Networks. *IEEE/ACM transactions on networking*, 2002, vol. 10, no. 3, pp. 411-424.
24. Alekhin S. V., Voitkevich K. L. *Modelirovanie protokola marshrutizatsii dlia besprovodnykh mobil'nykh setei* [Routing Protocol's Simulation for Wireless Mobile Networks]. *Telecommunications and Radio Engineering*, 2014, no. 7, pp. 7-8 (in Russian).
25. Voytkevich K. L., Sulima A. A., Zats P. A. Problemy postroeniia kanala upravleniia bespilotnymi letatel'nymi apparatami na osnove DKMV-radiolinii [The Problem of Constructing a Control Channel of Unmanned Aerial Vehicles Based on DKMV -Radio]. *Telecommunications and Radio Engineering*, 2014, no. 7, pp. 9-11 (in Russian).

26. Voytkevich K. L., Rezvov A. V., Shanin V. N. Spetsializirovannye lokal'nye besprovodnye mobil'nye seti grazhdanskogo i voennogo naznacheniiia [Specialized Local Wireless Mobile Networks for Civil and Military Purposes]. *Sistemy i sredstva sviazi, televideniia i radioveshchaniia*, 2013, № 1-2, pp. 130-133 (in Russian).

27. Komiakov A. V., Voytkevich K. L., Sulima A. A. Innovatsionnye resheniia dlia perspektivnykh letatel'nykh apparatov [Innovative Solutions for Advanced Aircraft]. *The inter-industry almanac "Delovaia slava Rossii"*, 2013, vol. 41, no. 3, pp. 26-27 (in Russian).

28. Belousov Ye. L., Bryantsev V. Ph., Voytkevich K. L., Keystovich A. V., Sayphetdinov Kh. I. Voprosy sozdaniia aviatsionnogo radiosviaznogo oborudovaniia po printsipu «programmiruemoe radio» [Issues of Developing Aviation Radio Communication Equipment on "Software-Defined Radio" Principle]. *Nizhny Novgorod state technical university n.a. R.E. Alexeev*, 2012, vol. 95, no. 2, pp. 11-18 (in Russian).

29. Belousov Ye. L., Bryantsev V. Ph., Voytkevich K. L., Keystovich A. V., Sayphetdinov Kh. I. Perspektivnoe bortovoe oborudovanie seti aviatsionnoi radiosviasi [Advanced Airborne Equipment for the Aviation Radio Communication Network]. *Nizhny Novgorod state technical university n.a. R.E. Alexeev*, 2012, vol. 96, no. 3, p. 11 (in Russian).

30. Voytkevich K. L. Opyt po sozdaniuu bortovykh kompleksov sviazi dlia samoletov takticheskogo zvena upravleniia [Experience on Creation of Onboard Complexes of Communication for Planes of a Tactical Control Link.]. *Sistemy i sredstva sviazi, televideniia i radioveshchaniia*, 2009, no. 1-2, pp. 42-43 (in Russian).

31. Makarenko S. I. Adaptivnoe upravlenie skorostiami logicheskikh soedinenii v kanale radiosviasi mnozhestvennogo dostupa [Adaptive Control Speed Logical Connections in the Radio Multiaccess Channel]. *Information and Control Systems*, 2008, no. 6, pp. 54-58 (in Russian).

32. Prokhorov A. V., Bondar' D. S. Primenenie apparatury shirokopolosnogo radiodostupa v lokal'nykh setiakh sviazi i peredachi dannykh sistem upravleniia vozdushnym dvizheniem [Application of Means of Broadband Radio Access in Local Communication Networks and Data Transmission for Systems of Air Traffic Management]. *Nauchnyi vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta grazhdanskoi aviatsii*, 2012, no. 176, pp. 93-100 (in Russian).

33. Ivanov V. I. Tsentralizovannyi metod balansirovki nagruzki v nizkoorbital'noi sputnikovoi sisteme [The centralized load balancing method for low earth orbit satellite system]. *T-Comm*, 2014, no 4, pp. 38-42 (in Russian).

Статья поступила 12 августа 2015 г.

Информация об авторе

Аганесов Артур Валерьевич – соискатель ученой степени кандидата наук. Помощник начальника учебного отдела. ВУНЦ ВВС «ВВА имени проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: маршрутизация информационных потоков и ретрансляция сообщений в воздушно-космических сетях связи; Mesh-технологии. E-mail: aganesov.artur@yandex.ru

Адрес: Россия, 394064, г. Воронеж, ул. Старых Большевиков, д. 54а.

Quality of Service of Aerospace Network Based on Hierarchical and Decentralized Routing Protocols

Aganesov A. V.

Statement of the problem. The creation of the united aerospace networks makes it relevant tasks of routing and relaying of messages in it. Given the quality of service of traffic you need to ensure. Two variants of the structure of the aerospace network considered in earlier works by the author. The first variant is a hierarchical structure where all traffic air networks is routing through the satellite network. The second variant is the decentralized structure with the use of the Mesh technology for join of air networks and the routing of traffic by through the adjacent air networks. **The purpose** of this work is the analysis and comparison of bandwidth in these variants of structure of the aerospace network. **Used methods.** The aerospace network model based on the model of hierarchical routing and decentralized routing model of traffic are presented in the earlier papers of the author. The air network model based on the CSMA/CA protocol model. The satellite network model based on the S-Aloha model. **Novelty.** Comparative evaluation of the bandwidth of the aerospace network with hierarchical and decentralized routing and the original model are the novelty of the paper. **Practical relevance:** the bandwidth estimation are presented in this work will be used to inform protocols relay traffic in the global aerospace networks. These results will be used for software routers of aerospace communication networks, built by Mesh technology.

Keywords: satellite network, relay traffic, routing, satellite network, radio networks, S-Aloha, CSMA.

Information about Author

Aganesov Artur Valer'evich - Doctoral Student. Assistant of head of training department. Military Training and Research Center of the Air Force "Military Air Academy Named After Professor N. E. Zhukovsky and Ju. A. Gagarin". Field of research: traffic routing and message relay in aerospace communication networks; Mesh-networks. E-mail: aganesov.artur@yandex.ru

Address: Russia, 355000, Voronezh, Street of Old Bolsheviks, 54a.

УДК 623.624

Динамическая модель системы связи в условиях функционально–разноуровневого информационного конфликта наблюдения и подавления

Макаренко С. И.

Постановка задачи: совершенствование средств и способов преднамеренных дестабилизирующих воздействий на системы связи требует развития научно-методического аппарата моделирования эффектов таких воздействий. Для описания функционирования системы связи в условиях преднамеренных воздействий предложено использовать понятие «информационного конфликта» ранее используемого в теории радиоэлектронной борьбы. В статье показано, что создание комплексов дестабилизирующих воздействий связано с интеграцией классических средств радиоэлектронного подавления, средств информационно-технического воздействия, а также средств радиомониторинга и компьютерной разведки. С учетом того, что эти средства ориентированы на разные уровни модели OSI (Open System Interconnection Reference Model), требуется разработка многоуровневой динамической модели информационного конфликта. **Целью работы** является разработка динамической модели информационного конфликта системы связи с системой дестабилизирующих воздействий. При этом система связи рассматривается как сложная многоуровневая иерархическая система, а информационный конфликт декомпозируется на локальные конфликтные ситуации на каждом из уровней модели OSI. **Используемые методы.** При обосновании математического аппарата для моделирования информационного конфликта был проведен анализ моделей конфликтов на основе теории игр, теории марковских процессов, теории сетей Петри, теории активного управления. При разработке динамической модели информационного конфликта были использованы методы теории динамических систем и теории сложных иерархических систем. **Новизна.** Элементом новизны является то, что в разработанной модели информационного конфликта учитываются одноуровневые и разноуровневые функциональные отношения между элементами системы, а также представление системы связи в виде сложной иерархической модели, в которой выделены как отдельные уровни, соответствующие модели OSI, так и отдельные протоколы, для которых рассмотрен информационный конфликт с учетом его отражения на показатели качества связи. Показана принципиальная возможность синтеза новых классов воздействий, ориентированных на создание и развитие внутрисистемных противоречий между отдельными протоколами системы связи, а также новых многоуровневых воздействий, реализуемых на различных уровнях модели OSI. **Результаты и их значимость.** Модель информационного конфликта в системе связи может быть использована для разработки новых стратегий управления связью с учетом противодействия комплексному воздействию средств радиоэлектронного подавления, средств информационно-технического воздействия, а также средств радиомониторинга и компьютерной разведки. Также модель может быть использована для обоснования новых видов воздействий, реализующих скрытое функциональное подавление системы связи за счет создания и развития внутрисистемных противоречий между ее отдельными протоколами.

Ключевые слова: динамическая модель, система связи, иерархическая система, сложная система, информационно-техническое воздействие, информационный конфликт, радиоэлектронная борьба, информационное противоборство, модель OSI.

Актуальность

В настоящее время ведется формирование методологии теории информационного противоборства в технической сфере как закономерного развития и синтеза ранее разобобщенных теорий радиоэлектронной борьбы и информационной безопасности. Анализ работ специалистов, ведущих исследования в области информационного противоборства: Пирумова В. С.,

Костина Н. А., Комова С. А., Новикова Д. А., Чхартишвили А. Г., Гриняева С. Н., Бухарина С. Н., Цыганова В. В., Ковалева В. И., Малкова С. Ю., Манойло А. В., Денисова А. А., Почепцова Г. Г., Расторгуева С. П., Бочкаревой Ю. Г. показывает, что создание и развитие научно-методического аппарата информационного противоборства тесно связано с теорией конфликтов (конфликтологией).

Изначально научные основы конфликтологии развивались, как часть социологии и были ориентированы на изучение конфликтов в социальных группах и между индивидами. Позднее пришло понимание, что конфликт, как абстрактная модель противоборства систем с различными целями, является основополагающей силой в развитии и самоорганизации военных, экономических, социальных и организационно-технических процессов и систем.

Конфликт - специфический процесс взаимодействия двух или большего количества компонентов системы (или систем в целом), преследующих разные интересы. Если интересы взаимодействующих систем (сторон) противоположны, то говорят об антагонистическом конфликте, а само взаимодействие сторон трансформируется в столкновение интересов [1].

Конфликтология нашла широкое применение в теории военного управления для обоснования распределения сил и средств, а также выбора стратегии в военном конфликте. Достаточно полный анализ научно-методического аппарата моделирования и принятия решений в военных конфликтах представлен в работе Новикова Д. А. [2].

Необходимо отметить, что для исследования процессов антагонистического взаимодействия организационно-технических систем в условиях военного конфликта, связанного с нарушением доступности, целостности и конфиденциальности информации достаточно давно введено понятие «*информационный конфликт*». В подавляющем числе работ по информационному конфликту он рассматривается в контексте применения средств радиоэлектронной борьбы (РЭБ) с целью нарушения функций информационного обеспечения системы управления силами и оружием.

Информационный конфликт (в РЭБ) - процесс столкновения сторон на этапе добывания с помощью радиоэлектронных средств данных о состоянии, намерениях и действиях противостоящей стороны, каждая из которых стремится к упреждающему по отношению к противостоящей стороне решению задач разведки и предпринимает определенные действия по снижению возможностей противостоящих средств разведки при обеспечении независимости эффективности своей системы вооружений от вмешательства действий другой стороны. Информационный конфликт в РЭБ является характерной формой проявления взаимоотношений подсистем информационного обеспечения противостоящих сторон на разных иерархических уровнях. При этом информационный конфликт в общем случае декомпозируется на упорядоченную во времени совокупность отдельных локальных конфликтных противоборств, каждое из которых представляет собой конфликт строго определенного состава сторон, иерархического уровня

при фиксированных и неизменных направлении и содержании действий в рамках решения задач противоборствующих сторон [1].

Конфликтное противоборство сторон, в рамках решения одной, строго определенной задачи, называют *дуэлью* [1-3]. Таким образом, дуэль является основополагающим элементом конфликта в РЭБ.

Информационный конфликт в РЭБ в общем случае характеризуется свойственной ему иерархической структурой, соответствующей разным уровням добываемой (требуемой) информации, и, соответственно, уровням добывания, сбора и обработки данных о противоборствующей стороне. Низший физический уровень (или как часто встречается в литературе - «сигнальный» уровень) информационного конфликта, представляет собой противоборство радиоэлектронных систем с целенаправленным использованием ими различного рода электромагнитных излучений и воздействий на физическую инфраструктуру в интересах получения первичной информации о характеристиках и состоянии основных объектов противостоящей стороны или/и предотвращение возможности получения такой информации другой стороной [1].

Традиционно информационный конфликт в РЭБ соответствует предметной области в которой ведется борьба и рассматривается для систем:

- радиолокации;
- навигационного обеспечения;
- радио/радиотехнического мониторинга;
- технической и компьютерной разведки;
- оптического наблюдения;
- систем радиосвязи.

Информационный конфликт между системами радиоэлектронного подавления (РЭП) и системой радиосвязи, широко исследован в работах Зюко А. Г. [5], Максимова М. В. [6], Шустова Л.Н. [6, 13], Коржика В. И., Финка М. М., Щелкунова К. Н. [7], Тузова Г. И. [8], Палия А. И. [9], Перунова Ю. М., Мацукевича В. В., Васильева А. А. [10], Радзиевского В. Г. [11, 37], Сироты А. А. [37], Куприянова А. И. [12, 13, 14], Сахарова А. В. [12], Борисова В. И., Зинчука В. М. [15, 16], Лимарева А. Е., Немчилова А. В., Чаплыгина А. А. [16] Владимирова В. И. [3, 17-21], Семисошенко М. А. [22], Чуднова А. М. [23-25], Барашкова П. Н., Родимова А. П., Ткаченко К. А. [25], Бураченко Д. Л. [26], Кузнецова В. И. [27], Боговика А. В., Игнатова В. В. [28], Исакова Е. Е. [29], Одоевского С. М., Калюки В. И. [30], Николаева В. И., Фёдорова А. Е. [31, 32], Шабалина Е. А. [34], Радько Н. М., Мокроусова А. Н. [35], Мальцева Г. Н., Вознюка В. В., Туктамышева М. Р. [26].

Однако в данных работах рассматривается конфликт системы радиосвязи и системы РЭП, как правило, на одном уровне – физическом (сигнальном). Вместе с тем как показано в работах Стародубцева Ю. И., Бухарина В. В., Семенова С. С. [38-41] в настоящее время наблюдается уход информационного конфликта в системах связи из его традиционной сферы – радиосвязи, в глобальное телекоммуникационное пространство. При таком расширении понятия информационного конфликта применительно к системам связи, во-

первых, методология конфликта на физическом уровне может быть дополнена исследованиями стойкости телекоммуникационных систем к воздействию электромагнитных импульсов и СВЧ-излучения. Во-вторых, становится актуальным рассмотрение в рамках информационного конфликта систем связи всей совокупности информационно-технических воздействий (ИТВ), ранее традиционно рассматриваемых как часть информационного противоборства в технической сфере.

В настоящее время имеется ряд исследований по рассмотрению информационного конфликта в системах радиосвязи с учетом его развития на уровнях модели OSI выше физического в работах Владимирова В.И. [20, 21], Боговика А.В., Игнатова В.В. [28], Чуднова А.М. [25], а также в ранее опубликованных работах автора. Имеется большое количество работ по моделированию воздействия ИТВ на системы связи на канальном, сетевом и транспортном уровнях OSI. Однако, данные работы, как правило, выполнены в рамках развития методологии информационной безопасности и не рассматривают взаимодействие ИТВ и средств информационной защиты в качестве конфликта. Имеющиеся работы Новикова Д.А. [42-45], Чхартишвили А.Г. [42, 43, 45], Губанова Д.А. [45], Расторгуева С.П. [46], Ломако А.Г., Бирюкова Д.Н. [47-49], Остапенко Г.А. [50, 51], Прилепского В.В. [52], Толстых Н.Н., Павлова В.А., Воробьевой Е.И. [53], Асоскова А.Н., Малышевой И.Н. [54], Мистрова Л.Е. [55, 56], Козирацкого Ю.Л. [57-59], Будникова С.А. [60-63], Бойко А.А. [63-65], Храмова В.Ю. [64], Вялых А.С., Вялых С.А., Сироты А.А. [66, 67], Толстых Н.Н. [68-69], Стюгина М.А. [70-73], Шевцова В.А. [74], Чуклеяева И.И. [75, 76], Якушенко С.А. [77], Данаева А.В., Воробьева А.А. [78] в области информационного противоборства в рамках дуэли «информационно-управляющая система – система дестабилизирующих воздействий», как правило, рассматривают конфликт на одном уровне функционирования этих систем. При этом в работах Козирацкого Ю.Л. [1], Владимирова В.И. [3], Радзиевского В.Г., Сироты А.А. [37], Новикова Д.А. [44], Григорьева В.Р., Шуркина Л.О. [79] отмечается, что информационный конфликт носит сложный иерархический характер и может состоять из множества дуэльно-игровых ситуаций на различных уровнях иерархии.

Таким образом, анализ исследований в области информационного конфликта в рамках РЭБ, информационного противоборства и информационной безопасности показал, что требуется расширение понятия «информационный конфликт» на всю область информационного противоборства с включением в него методологии по конфликтам в области радиосвязи. При этом необходимо учесть, что объектами исследования теории информационного противоборства являются сложные иерархические информационно-управляющие метасистемы (государственного, политического, военного, социального и экономического назначения).

Как показано в работах Владимирова В.И. [3], Стародубцева Ю.И., Бухарина В.В., Семенова С.С. [38-41], Будникова С.А. [60], Антоновича П.И. [80], Паршуткина А.В. [81, 82], Чуклеяева И.И. [76] Якушенко С.А. [77]

методология развития информационного противоборства в технической сфере связана с интеграцией «классических» средств РЭП и новых способов ИТВ.

В известных работах по конфликтам в области информационного противоборства: Новикова Д.А. [42-45], Чхартисвили А.Г. [42, 43, 45], Губанова Д.А. [45], Расторгуева С.П. [46], Ломако А.Г., Бирюкова Д.Н. [47-49], Остапенко Г.А. [50, 51], Козирацкого Ю.Л. [57-59], Будникова С.А. [60-63], как правило, основной упор делается на особенности стратегий участников. При этом в работах по информационному конфликту систем связи отсутствует его согласование с моделью OSI (Open System Interconnection Reference Model).

Имеются работы в области анализа функционирования комплексов связи и управления как многоуровневых иерархических систем Цвиркуна А.Д. [83], Гуревича И.М. [84, 85], Агеева Д.В. [86, 87], Илюхина А.А. [88, 89], Маслобоева А.В., Путилова В.А., Сютин А.В. [90]. Однако в них не рассматриваются конфликтные ситуации характерные для информационного противоборства.

В работах Паршуткина А. В. [81, 82] представлено развитие модели информационного конфликта «классического» РЭП и систем радиосвязи в направлении повышения «многоуровневости» конфликта и согласования его с моделью OSI. Данные работы предлагают совместно с «классическим» информационным конфликтом со средствами РЭП учесть новые способы ИТВ за счет декомпозиции информационного конфликта системы связи на отдельные конфликтные ситуации на каждом из уровней модели OSI (рис. 1). Таким образом, предложенный в работах Паршуткина А.В. [81, 82] новый концептуальный подход к моделированию информационного конфликта, с одной стороны органично развивает существующие работы Козирацкого Ю.Л. [1], Владимирова В.И. [3], Радзиевского В.Г. [11] в области многоуровневого информационного конфликта радиоэлектронных систем, а с другой – формализует конфликтное взаимодействие в соответствии с уровнями эталонной модели OSI. Данная концептуальная модель, названная автором *эталонной моделью взаимодействия конфликтующих систем CSI (Conflict System Interconnection Reference Model)* формализует объекты и общие подходы к описанию локальных информационных конфликтов в системе связи на каждом из уровней модели OSI. В модели CSI подразумевается, что средствами вскрытия и наблюдения протоколов, используемых в системах связи, останутся «классические» средства радиоэлектронной и компьютерной разведки, а средствами подавления – как «традиционные» средства РЭП, так и новые виды ИТВ.

Известные работы в области информационного конфликта основываются на научно-методическом аппарате:

- теории активных систем (работы Новикова Д.А., Чхартисвили А.Г. [42, 43, 45], Губанова Д.А. [45], Расторгуева С.П. [46]);
- теории игр (работы Семисошенко М.А. [22], Чуднова А.М. [24, 25], Одоевского С.М., Калюки В.И. [30], Чукляева И.И. [75], Якушенко С.А. [77]);

- марковских процессов (работы Козирацкого Ю.Л., Владимирова В.И. [3, 20, 21], Лихачева В.П., Шляхина В.М. [21], Радзиевского В. Г., Сироты А.А. [37], Будникова С.А. [1, 60, 62]);
- многоагентных интеллектуальных систем (работы Бирюкова Д.Н., Ломако А.Г. [47-49], Гриняева С.Н. [91]);
- теории сетей Петри (работы Радько Н.М. [35], Мальцева Г.Н., Туктамышева М.Р. [36], Будникова С.А. [62]);
- теории автоматов (работа Девянина Н.П. [95]);
- вероятностные сети (работы Коцыняк М.А., Лауты О.С. [96-97]);
- теории динамических систем (работы Григорьева В.Р., Шуркина Л.О. [79], Гуревича И.М. [84, 85, 92, 93]);
- теории сложных иерархических систем (работы Козирацкого Ю.Л., Будникова С.А. [1], Владимирова В.И. [3], Радзиевского В.Г., Сироты А.А. [37], Новикова Д.А. [44, 98], Месаровича М., Такахары И. [99, 100]).

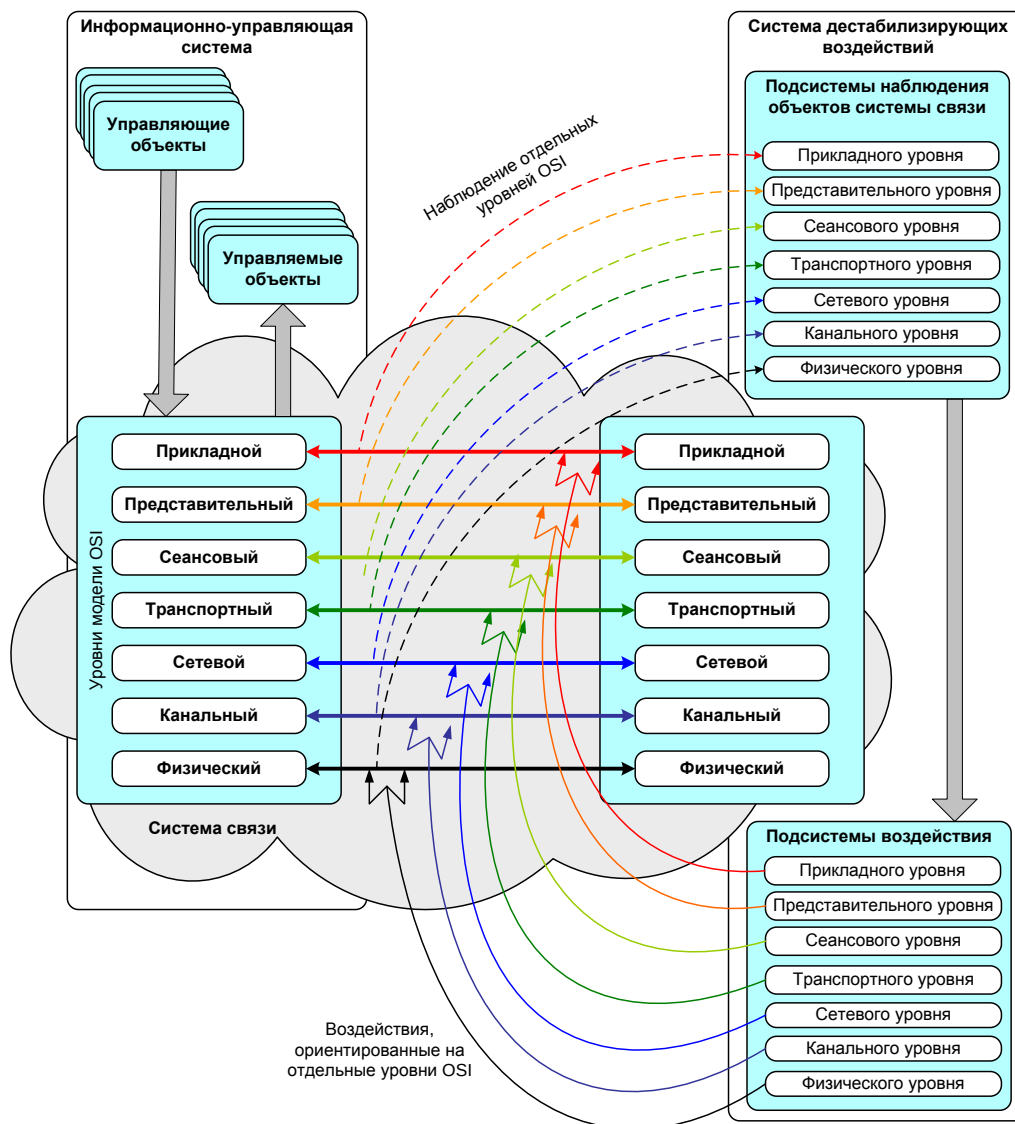


Рис. 1. Модель CSI

В статье рассматривается информационный конфликт в системе связи формализованный на основе теории динамических систем, в терминологии работ [101, 102, 103] и представленный в виде многоуровневой иерархической динамической модели. При этом ее отдельные уровни соответствуют модели CSI, предложенной Паршуткиным А.В. [81, 82], а за концептуальную основу модели системы связи взята двухуровневая модель, представленная в работе [25]. В качестве более ранних работ, которые частично послужили прототипами общего подхода к моделированию иерархического динамического конфликта в системах связи, относятся работы Гуревича И.М. [84, 85, 92, 93], Вакуленко А.А., Шевчука В.И. [104], Маевского Ю.И. [105], Поповского В.В., Лемешко А.В., Евсеевой О.Ю. [106].

Постановка задачи

Для формализации модели введем следующие обозначения.

1) Элементы системы:

$l=1\ldots 7$ – номер уровня функционирования системы связи в соответствии с моделью OSI;

π – протокол связи;

π_l – протокол связи на l -ом уровне функционирования;

$\pi_{l,i}$ – i -ый протокол связи на l -ом уровне;

$\Pi_l = \bigcup_i \{\pi_{l,i}\}$ – множество протоколов связи, используемых в системе связи, на l -ом уровне ее функционирования;

$\Pi_{l,v} = \bigcup_i \{\pi_{l,i} \mid V_l \in X_{l,\pi}\}$ – множество протоколов связи, используемых на l -ом уровне и подвергающихся преднамеренному дестабилизирующему воздействию V_l ;

$\Pi = \bigcup_l \Pi_l$ – множество протоколов связи используемых в системе связи на всех уровнях ее функционирования;

a – элемент математического обеспечения (алгоритм) используемый в системе связи;

$A_{l,\pi} = \{a \mid a \in D(\pi_l)\}$ – множество элементов математического обеспечения (алгоритмов), реализующих функционирование π -го протокола на l -ом уровне функционирования системы связи;

$D(\cdot)$ – область определения ($\cdot$);

$A_l = \bigcup_{\pi_l} A_{l,\pi}$ – множество элементов математического обеспечения (алгоритмов), реализующих функционирование протоколов Π_l на l -ом уровне системы связи;

$A = \bigcup_l A_l$ – множество элементов математического обеспечения (алгоритмов) системы связи;

ω – параметр элемента математического обеспечения (алгоритма) a ;

$\Omega_{l,\pi,a} = \{\omega \mid \omega \in D(a), a \in D(\pi_l)\}$ – множество параметров a -го математического обеспечения (алгоритма) π -го протокола на l -ом уровне системы связи;

$\Omega_{l,\pi} = \bigcup_{\pi} \Omega_{l,\pi,a}$ – множество параметров математического обеспечения (алгоритмов) π -го протокола связи на l -ом уровне системы связи;

$\Omega_l = \bigcup_{\Pi_l} \Omega_{l,\pi}$ – множество параметров математического обеспечения (алгоритмов) протоколов Π_l на l -ом уровне системы связи;

$\Omega = \bigcup_l \Omega_l$ – множество параметров математического обеспечения (алгоритмов) на всех уровнях системы связи;

r – отдельный вид ресурса системы связи;

$R_{l,\pi} = \{r \mid r \in D(\pi_l)\}$ – ресурс системы связи на l -ом уровне ее функционирования используемый для функционирования π -го протокола;

$R_l = \bigcup_{\Pi_l} R_{l,\pi}$ – ресурс системы связи на l -ом уровне ее функционирования, используемый для функционирования протоколов Π_l и организации связи;

$R = \bigcup_l R_l$ – ресурс системы связи на всех уровнях ее функционирования;

$R_{l,V} = \{r \mid r \in D(V_l), r \in R_l\}$ – ресурс на l -ом уровне функционирования системы связи, используемый системой дестабилизирующих воздействий для V_l -го воздействия на протоколы связи Π_l ;

$Z = \{z_i\}$ – множество узлов системы связи;

$E = \{e_i\}$ – множество средств связи, установленных на узлах сети связи;

$K = \{k_{ij}\}$ – множество каналов связи, соединяющих узлы сети связи (средства связи). Предполагается, что канал k_{ij} соединяет узлы z_i и z_j в случае если средства связи e_i и e_j , размещенные на этих узлах, используют совместный протокол связи $\pi_{l,k}$;

$\Theta_{l,\pi} = \{(a_{l,\pi,i}, a_{l,\pi,j})\}$, $i, j = 1 \dots |A_{l,\pi}|$ – множество функциональных связей между алгоритмами $A_{l,\pi}$ в протоколе π_l на l -ом уровне системы связи;

$|\cdot|$ – количество элементов в множестве ($\cdot$);

$\Theta_l = \{(\pi_{l,i}, \pi_{l,j})\}$, $i, j = 1 \dots |\Pi_l|$ – множество функциональных связей между протоколами $\pi_l \in \Pi_l$ на l -ом уровне системы связи;

$\Theta = \{(\pi_{l_1,i}, \pi_{l_2,j})\}$, $i, j = 1 \dots |\Pi_l|$, $l_1, l_2 = 1 \dots 7$ – множество функциональных связей между протоколами $\pi_l \in \Pi$ в системе связи на различных ее уровнях;

s_π – состояние π -го протокола связи;

$S_{l,\pi} = \{s_\pi\}$ – множество состояний π_l -го протокола связи на l -ом уровне функционирования системы связи;

$S_l = \{S_{l,\pi}\} \cup \Theta_l$ – множество состояний l -ого уровня функционирования системы связи, определяемое состояниями протоколов и связями между ними;

$S = \langle t_0, t, \{S_l\}, X, U, A, \Theta, Z, E, K, \Lambda \rangle$ – множество состояний системы связи;

$S_{conf} = \langle t, R, \Omega, A, \Theta, Z, K, \Lambda \rangle$ – конфигурация системы связи, определяющая ее текущую структуру и множество функциональных связей;

$S_{conf}^{набл} = \{\langle t, R, \Omega, A, \Theta, Z, K, \Lambda \rangle\} \in M$ – конфигурация системы связи, наблюдаемая со стороны системы дестабилизирующих воздействий;

Λ – информационная структура системы связи, определяющая маршруты циркуляции информационных потоков;

2) Параметры и показатели системы:

q – отдельный показатель качества (QoS – Quality of Service) функционирования системы связи;

$Q_{l,\pi} = \{q \mid q \in E(\pi_l)\}$ – множество показателей QoS системы связи на l -ом уровне, которые обеспечивает π_l -ый протокол связи;

$E(\cdot)$ – область значений ($\cdot$);

$Q_{l,\pi,N} = \{q \mid q \in Q_{l,\pi}, q \in N_{l,\pi}\}$ – множество показателей QoS системы связи на l -ом уровне, которые обеспечивает π_l -ый протокол связи наблюдаемые системой управления связи по каналу наблюдения $N_{l,\pi}$;

$Q_{l,\pi,M} = \{q \mid q \in Q_{l,\pi}, q \in M_{l,\pi}\}$ – множество показателей QoS системы связи на l -ом уровне, которые обеспечивает π_l -ый протокол связи наблюдаемые системой дестабилизирующих воздействий по каналу наблюдения $M_{l,\pi}$;

$Q_{l,\pi,V} = \{q_{l,\pi} \mid q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$ – множество показателей QoS системы связи на l -ом уровне, которые обеспечивает π_l -ый протокол связи которые снижаются в результате преднамеренных дестабилизирующих воздействий $V_{l,\pi}$;

$Q_l = \bigcup_{\pi_l} Q_{l,\pi}$ – множество показателей QoS системы связи на l -ом уровне;

$Q_{l,N} = \bigcup_{\pi_l} Q_{l,\pi,N}$ – множество показателей QoS системы связи на l -ом уровне, наблюдаемые системой управления связи по каналу наблюдения N_l ;

$Q_{l,M} = \bigcup_{\pi_l} Q_{l,\pi,M}$ – множество показателей QoS системы связи на l -ом уровне, наблюдаемые системой дестабилизирующих воздействий по каналу наблюдения M_l ;

$Q = \bigcup_l Q_l$ – множество показателей QoS системы связи на всех ее уровнях;

$Q_N = \bigcup_l Q_{l,N}$ – множество показателей QoS системы связи на всех ее уровнях наблюдаемые системой управления связи по каналу наблюдения N ;

$Q_M = \bigcup_l Q_{l,M}$ – множество показателей QoS системы связи на всех ее уровнях наблюдаемые системой дестабилизирующих воздействий по каналу наблюдения M ;

t – время функционирования системы связи;

t_0 – начальный момент функционирования системы связи;

$t_{\text{тек}}$ – текущий момент функционирования системы связи;

$t_{\text{набл}}$ – интервал времени наблюдения;

T – множество моментов времени функционирования системы связи (непрерывных или дискретных);

T_η – множество моментов времени наблюдения элементов системы связи со стороны системы управления связью;

T_U – множество моментов времени выдачи управляющих воздействий на элементы системы связи со стороны системы управления связью;

T_V – интервал времени в течении которых дестабилизирующих воздействий на элементы системы связи со стороны противника;

k_u – показатель устойчивости системы связи;

3) Связи внутри системы:

η – параметр, наблюдаемый со стороны системы управления связью;

$N_{l,\pi} = \{\eta \mid \eta \in E(\pi_l), \eta \in \langle Q_{l,\pi} \times Y_{l,\pi} \rangle\}$ – канал наблюдения выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на своем l -ом уровне системы связи со стороны системы управления связью;

$N_l = \bigcup_{\pi_l} N_{l,\pi}$ – канал наблюдения параметров Y_l и показателей QoS Q_l на l -ом уровне системы связи со стороны системы управления связью;

$N = \bigcup_l N_l$ – канал наблюдения параметров Y и показателей QoS Q на всех уровнях системы связи со стороны системы управления связью;

μ – параметр, наблюдаемый со стороны системы управления воздействиями противника;

$M_{l,\pi} = \{\mu \mid \mu \in E(\pi_l), \mu \in \langle Q_{l,\pi} \times Y_{l,\pi} \rangle\}$ – канал наблюдения выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на своем l -ом уровне системы связи со стороны системы дестабилизирующих воздействий;

$M_l = \bigcup_{\pi_l} M_{l,\pi}$ – канал наблюдения параметров Y_l и показателей QoS Q_l на l -ом уровне системы связи со стороны системы дестабилизирующих воздействий;

$M = \bigcup_l M_l$ – канал наблюдения параметров $\{Y_l\}$ и показателей QoS Q на всех уровнях системы связи со стороны системы дестабилизирующих воздействий;

v – отдельное воздействие со стороны системы дестабилизирующих воздействий;

$V_{l,\pi} = \{v \mid v \in D(\pi_l), v \in \langle R_{l,\pi} \times \Omega_{l,\pi} \times A_{l,\pi} \times \Theta_{l,\pi} \rangle\}$ – множество воздействий со стороны системы дестабилизирующих воздействий на протокол π_l , функционирующий на l -ом уровне системы связи;

$V_l = \bigcup_{\pi_l} V_{l,\pi}$ – множество воздействий осуществляемых на l -ый уровень системы связи со стороны системы дестабилизирующих воздействий;

$V = \bigcup_l V_l$ – множество воздействий осуществляемых на все уровни системы связи со стороны системы дестабилизирующих воздействий;

$\chi_{l,\pi}$ – множество параметров естественной среды функционирования системы связи (без преднамеренных дестабилизирующих воздействий), определяющие параметрическое пространство для протокола π_l на l -ом уровне;

$\chi_l = \bigcup_{\pi_l} \chi_{l,\pi}$ – множество параметров естественной среды функционирования системы связи, определяющие параметрическое пространство для протоколов Π_l на l -ом уровне;

$\chi = \bigcup_l \chi_l$ – множество параметров естественной среды функционирования системы связи;

$X_{l,\pi} = \langle \chi_{l,\pi} \times R_{l,\pi} \times V_{l,\pi} \rangle$ – множество параметров среды, определяющих параметрическое пространство для протокола π_l системы связи на l -ом уровне функционирования с учетом выделяемых протоколу на l -ом уровне ресурсов $R_{l,\pi}$, параметров естественной среды $\chi_{l,\pi}$ и множества $V_{l,\pi}$ преднамеренных дестабилизирующих воздействий на этот протокол;

$X_l = \bigcup_{\pi_l} X_{l,\pi} = \langle \chi_l \times R_l \times V_l \rangle$ – множество параметров среды, определяющих параметрическое пространство для протоколов системы связи Π_l на l -ом уровне функционирования, с учетом ресурсов l -ого уровня R_l , параметров естественной среды χ_l и множества V_l дестабилизирующих воздействий на этом уровне;

$X = \bigcup_l X_l = \langle \chi \times R \times V \rangle$ – множество параметров среды, определяющих параметрическое пространство для системы связи на всех ее уровнях, с учетом ее ресурсов R , параметров естественной среды χ и всего множества дестабилизирующих воздействий V ;

u – управляющее воздействие на элемент системы связи со стороны системы управления связью;

$u_{l,\pi}$ – управляющее воздействие на протокол π_l системы связи со стороны системы управления связью на l -ом уровне функционирования;

$U_{l,\pi} = \langle u_{l,\pi} \times T \rangle$ – функционал, задающий множество управляющих воздействий (управление) на протокол π_l , со стороны системы управления связью на l -ом уровне с целью обеспечения протоколом требуемых показателей QoS $Q_{l,\pi}$;

$U_l = \bigcup_{\pi_l} U_{l,\pi}$ – функционал задающий множество управляющих воздействий (управление) на протоколы Π_l l -ого уровня со стороны системы управления связью на этом уровне с целью обеспечения требуемых показателей QoS Q_l ;

$U = \bigcup_l U_l$ – функционал, задающий множество управляющих воздействий (управление) на протоколы Π всех уровней со стороны системы управления связью с целью обеспечения требуемых показателей QoS Q ;

y – выходной параметр протокола системы связи;

$Y_{l,\pi} = \{y \mid y \in E(\pi_l)\}$ – множество выходных параметров π_l -го протокола на l -ом уровне системы связи;

$Y_{l,\pi,N} = \{y \mid y \in Y_{l,\pi}, y \in N_{l,\pi}\}$ – множество выходных параметров π_l -го протокола на l -ом уровне наблюдаемые системой управления связью по каналу наблюдения $N_{l,\pi}$;

$Y_{l,\pi,M} = \{y \mid y \in Y_{l,\pi}, y \in M_{l,\pi}\}$ – множество выходных параметров π_l -го протокола на l -ом уровне, наблюдаемые системой дестабилизирующих воздействий по каналу наблюдения $M_{l,\pi}$;

$Y_l = \bigcup_{\pi_l} Y_{l,\pi}$ – множество выходных параметров l -ого уровня системы связи;

$Y_{l,N} = \bigcup_{\pi_l} Y_{l,\pi,N}$ – множество выходных параметров l -ого уровня системы связи, наблюдаемые системой управления связью по каналу наблюдения N_l ;

$Y_{l,M} = \bigcup_{\pi_l} Y_{l,\pi,M}$ – множество выходных параметров l -ого уровня системы связи, наблюдаемые системой дестабилизирующих воздействий по каналу наблюдения M_l ;

$Y_N = \bigcup_l Y_{l,N}$ – множество выходных параметров всех уровней системы связи, наблюдаемые системой управления связью по каналу наблюдения N ;

$Y_M = \bigcup_l Y_{l,M}$ – множество выходных параметров всех уровней системы связи, наблюдаемые системой дестабилизирующих воздействий по каналу наблюдения M ;

$Y = \bigcup_l Y_l$ – множество выходных параметров системы связи;

Y_l – конечные выходные параметры системы связи;

$\psi_{l,\pi}$ – отображение, задающее смену состояний $s_\pi \in S_\pi$ протокола π_l на l -ом уровне функционирования;

ψ_l – отображение, задающее смену состояний $s_l \in S_l$ l -ого уровня системы связи;

ψ – отображение, задающее смену состояний $s \in S$ системы связи;

$f_{l,\pi}$ – отображение, определяющее выходные показатели качества обслуживания $Q_{l,\pi}$, которые обеспечивает протокол π_l на своем l -ом уровне функционирования;

f_l – отображение, определяющее выходные показатели качества обслуживания Q_l , которые обеспечивают множество протоколов Π_l на l -ом уровне функционирования;

f – отображение, определяющее выходные показатели качества обслуживания Q системы связи;

$\gamma_{l,\pi}$ – отображение, определяющее выходные параметры Y_π протокола π_l на l -ом уровне;

γ_l – отображение, определяющее выходные параметры Y_l множества протоколов Π_l на l -ом уровне;

γ – отображение, определяющее выходные параметры Y системы связи;

$\varphi_{l,\pi}$ – отображение, определяющее параметрическое множество среды функционирования протоколов более высокого уровня X_{l+1} зависимое от протокола π_l на l -ом уровне;

φ_l – отображение, определяющее параметрическое множество среды функционирования X_{l+1} протоколов более высокого уровня Π_{l+1} ;

$\varphi = \bigcup_l \varphi_l$ – множество отображений, определяющих межуровневые связи между уровнями системы связи.

Задачей работы является формализация информационного конфликта как для отдельных протоколов на конкретных уровнях модели OSI, так и для системы связи в целом, учитывая ее взаимодействие с системой дестабилизирующих воздействий в виде единой многоуровневой иерархической динамической модели.

Модель протокола системы связи на отдельном уровне функционирования

В отличие от известных моделей представленных в работах Барашкова П.Н., Родимова А.П., Ткаченко К.А., Чуднова А.М.. [25] и Боговика А.В., Игнатова В. В. [28] в данной модели системы связи к основному элементу системы связи предложено отнести протокол связи π как ее функционально-простейший элемент.

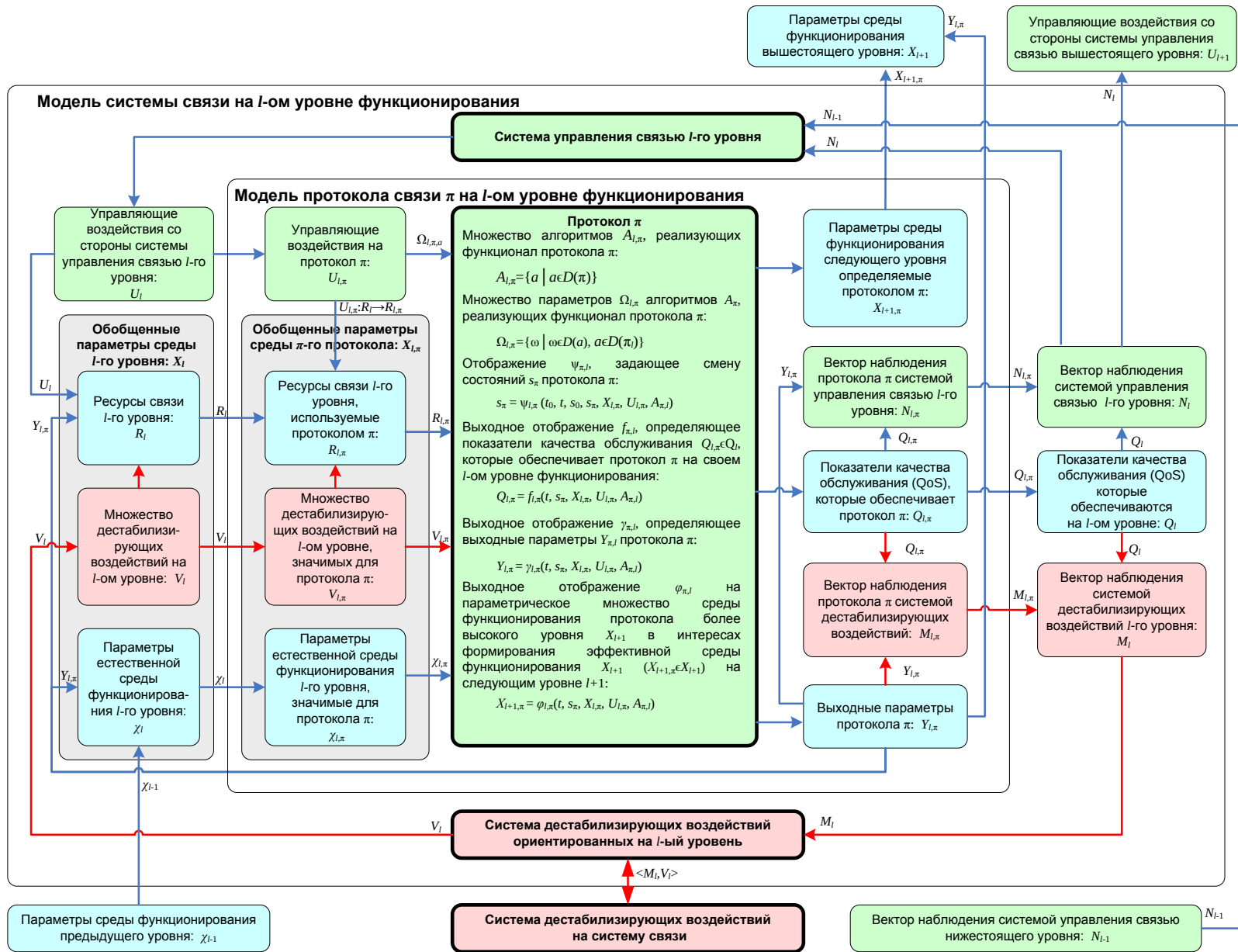


Рис. 2. Модель отдельного протокола при информационном конфликте, в виде динамической системы

При этом под *протоколом* понимается формализованный набор правил, задаваемых математическим обеспечением протокола, а также их параметров, которые позволяют осуществлять соединение и обмен данными между двумя или более абонентами. Функционально протоколы классифицируются в соответствии с уровнями модели OSI. Причем протоколы физического уровня реализуются аппаратно, протоколы канального и сетевого уровня – аппаратно-программными средствами, а протоколы транспортного уровня и выше – программно.

Рассмотрим общую модель протокола (рис. 2), построенную как динамическую модель на основе теории систем [99-102].

В общем случае модель протокола π_l в виде динамической системы описывается следующими параметрами и отображениями.

1) Входные параметры:

- множество обобщенных параметров среды $X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle$, в которой функционирует протокол π_l на l -ом уровне, включающие в себя:
 - множество параметров естественной среды l -го уровня $\chi_{l,\pi}$, значимые для протокола π_l (при этом $\chi_{l,\pi} \subseteq \chi_l \subseteq \chi$);
 - множество ресурсов связи l -го уровня $R_{l,\pi}$, используемых протоколом π_l (при этом $R_{l,\pi} \subseteq R_l \subseteq R$);
 - множество преднамеренных воздействий $V_{l,\pi}$ реализуемых системой дестабилизирующих воздействий на l -ом уровне и влияющих на функционирование протокола π_l ($V_{l,\pi} \subseteq V_l \subseteq V$);
- множество управляющих воздействий $U_{l,\pi} = \langle u_{l,\pi} \times T \rangle$ ($U_{l,\pi} \subseteq U_l \subseteq U$) на протокол π_l , со стороны системы управления связи на l -ом уровне, заключающиеся в рациональном распределении ресурсов l -ого уровня ($u_{l,\pi}: R_l \rightarrow \{R_{l,\pi}\}$) и в управлении параметрами $\Omega_{l,\pi}$ функционирования протокола π_l с целью обеспечения требуемого качества обслуживания: $u_{l,\pi}: \Omega_{l,\pi,a} \rightarrow Q_{l,\pi} \mid \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}$;
- множество моментов времени функционирования системы связи T .

2) Отображения, определяющие общую динамическую модель протокола π_l на l -ом уровне:

- множество алгоритмов $A_{l,\pi}$, реализующих функционал протокола π_l , связанных между собой в соответствии со структурой $\Theta_{l,\pi}$:

$$A_{l,\pi} = \{a \mid a \in D(\pi_l)\};$$

$$\pi_l = A_{l,\pi} \cup \Theta_{l,\pi}; \quad (1)$$

- множество параметров $\Omega_{l,\pi,a}$ алгоритмов $A_{l,\pi}$, реализующих функционал протокола π_l :

$$\Omega_{l,\pi,a} = \{\omega \mid \omega \in D(a), a \in D(\pi_l)\}; \quad (2)$$

- отображение $\psi_{l,\pi}$, задающее смену состояний s_π ($s_\pi \in S_{l,\pi}$) протокола π_l :

$$s_\pi = \psi_{l,\pi}(t_0, t, s_\pi(t_0), S_{l,\pi}, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}); \quad (3)$$

- отображение $f_{l,\pi}$, определяющее выходные показатели качества обслуживания $Q_{l,\pi} \in Q_l$, которые обеспечивает протокол π_l на l -ом уровне функционирования:

$$Q_{l,\pi} = f_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}); \quad (4)$$

- отображение $\gamma_{l,\pi}$, определяющее выходные параметры $Y_{l,\pi}$ протокола π_l :

$$Y_{l,\pi} = \gamma_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}); \quad (5)$$

- отображение $\varphi_{l,\pi}$, определяющее параметрическое множество среды функционирования протоколов более высокого уровня X_{l+1} :

$$X_{l+1,\pi} = \varphi_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}). \quad (6)$$

3) Выходные параметры:

- множество выходных параметров $Y_{l,\pi}$ протокола π_l ;
- множество показателей качества обслуживания $Q_{l,\pi} \in Q_l$, которые обеспечивает протокол π_l на l -ом уровне функционирования;
- множество параметров среды функционирования протоколов более высокого уровня $X_{l+1,\pi}$ ($X_{l+1,\pi} \subseteq X_{l+1}$). Фактически данный выходной параметр определяет возможности протокола текущего уровня по исправлению ошибок и негативных воздействий входного параметра предыдущего уровня (например, система радиоэлектронной защиты при приеме сигналов X_1 осуществляет фильтрацию помех, и преобразовывает сигналы в двоичный код X_2 , на 2-ом уровне битовый поток X_2 объединяется в блоки, в которых на основе схемы помехоустойчивого кодирования исправляются ошибки, и исправленный блок передается на сетевой уровень X_3 и т.д.).
- канал наблюдения $N_{l,\pi}$ выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на l -ом уровне системы связи со стороны системы управления связью:

$$N_{l,\pi} = \{\eta \mid \eta \in \mathbf{E}(\pi_l), \eta \in \langle Q_{l,\pi} \times Y_{l,\pi} \rangle\},$$

$\mathbf{E}(\cdot)$ – область значений ($\cdot$);

- канал наблюдения $M_{l,\pi}$ выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l на l -ом уровне системы связи со стороны системы дестабилизирующих воздействий (средствами радиотехнической и радиоразведки, а также другими средствами мониторинга) в интересах принятия решений по применению воздействий $V_{l,\pi}$:

$$M_{l,\pi} = \{\mu \mid \mu \in \mathbf{E}(\pi_l), \mu \in \langle Q_{l,\pi} \times Y_{l,\pi} \rangle\}.$$

Параметры $R_{l,\pi}$, $V_{l,\pi}$, $U_{l,\pi}$ представляют собой конечномерные векторные функции от времени t , $t \in T$. Множество параметров естественной среды $\chi_{l,\pi}$ может быть как функциями от времени t (например, медленные или быстрые замирания при распространении радиосигналов коротких волн, зависящие от времени суток или сезона), так и случайными параметрами, как правило, с нормальным или экспоненциальным распределением (например, мощность аддитивного белого гауссовского шума или плотность вероятности наработки на

отказ оборудования связи). Таким образом, модель протокола π_l представляет собой конечномерную динамическую систему, определенную на параметрическом пространстве $R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \times U_{l,\pi} \times T$ и заданную отображениями $\Psi_{l,\pi}, f_{l,\pi}, \gamma_{l,\pi}, \varphi_{l,\pi}$.

Рассмотрим особенности функционирования отдельного протокола более подробно.

Процесс функционирования протокола π_l определяется отображением $\gamma_{l,\pi}: \langle t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi} \rangle \rightarrow Y_{l,\pi}$ задаваемым выражением (5), в процессе которого производится выработка множества выходных параметров $Y_{l,\pi}$ которые соответствуют целевому назначению протокола, в зависимости от текущего состояния протокола s_π и входных воздействий $\langle X_{l,\pi}, U_{l,\pi} \rangle$.

Выполнение функций по целевому назначению протокола π_l ведется по заложенному в него множеству алгоритмов $A_{l,\pi} = \{a \mid a \in D(\pi_l)\}$, взаимоувязанных в единую систему в соответствии со структурой связей $\Theta_{l,\pi}$. Функционирование алгоритмов $A_{l,\pi}$, в свою очередь, зависит от их собственных параметров $\Omega_{l,\pi,a} = \{\omega \mid \omega \in D(a), a \in D(\pi_l)\}$ и параметров среды $X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle$. Для выполнения целевых задач протоколу π_l выделяются ресурсы $R_{l,\pi}$. Контроль качества функционирования ведется по значениям показателей QoS $\{q_{l,\pi}\} \in Q_{l,\pi}$, которые обеспечивает этот протокол.

Оценкой качества функционирования протокола π_l является множество показателей QoS $Q_{l,\pi}$, которые определяются в соответствии с выражением (4). В интересах обеспечения заданного уровня показателей QoS $\{q_{l,\pi}^{\text{треб}}\}$ на протокол π_l со стороны системы управления связью оказывается множество управляющих воздействий $U_{l,\pi}$, которые, как правило, связаны или с распределением ресурсов $R_{l,\pi}$ доступных протоколу π_l , или с изменением параметров $\Omega_{l,\pi,a}$ алгоритмов $A_{l,\pi}$, на основе которых функционирует протокол.

Например, протокол детектирования и помехоустойчивого приема сигналов может обеспечивать в качестве множества $Y_{l,\pi}$ следующие сигнальные параметры: вероятность правильного обнаружения сигнала, мощность сигнала, вид модуляции, различные энергетически-временные параметры, цифровая последовательность, соответствующая принятому сигналу и т.д. Для этого протокола под множеством $A_{l,\pi}$ можно рассматривать: алгоритм обнаружения сигнала, алгоритмы когерентного и некогерентного приема. Под множеством параметров $\Omega_{l,\pi,a}$ алгоритмов $A_{l,\pi}$ – критерий обнаружения и порог для него, время накопления сигнала, пороговое значение автокорреляционной функции и др. В качестве ресурса $R_{l,\pi}$ можно рассматривать частотно-временную область, в которой ведется прием сигналов. В качестве параметров естественной среды $\chi_{l,\pi}$ – значение отношения мощности сигнала к мощности шума (ОСШ) на входе приемника в условиях отсутствия помех и энергетически-временные параметры принимаемого сигнала. В качестве дестабилизирующего воздействия $V_{l,\pi}$ – воздействие средств РЭП, снижающие значение ОСШ и, как следствие, понижающие показатели QoS $Q_{l,\pi}$ протокола приема. В качестве элементов множества показателей QoS $Q_{l,\pi}$ могут выступать: вероятность правильного обнаружения сигнала, вероятность ошибочного

приема сигнала, вероятность ошибки на бит, пропускная способность канала и др.

Качество функционирования протокола определяется соответствием всех показателей QoS из множества $Q_{l,\pi}$ критерию эффективности (7).

Протокол является эффективно функционирующим в случае, если все его показатели качества $\forall \{q_{l,\pi}\} \in Q_{l,\pi}$, которые он обеспечивает, имеют значения не ниже требуемого, то есть выполняется критерий:

$$\forall \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}. \quad (7)$$

Функционирование протокола π_l , как правило, сопровождается динамическим или стохастическим изменением значений множества параметров среды функционирования $X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle$, которые в условиях противоборства в первую очередь определяются множеством дестабилизирующих воздействий $V_{l,\pi}$.

Условимся называть множество входных параметров $X_{l,\pi} \times U_{l,\pi}$ *эффективным*, если оно позволяет обеспечить выполнение критерия эффективного функционирования протокола (7), и *неэффективным* – если не позволяет.

Для обеспечения соответствия критерия (7) заданным значениям на протокол π_l со стороны системы управления связью оказывается множество управляющих воздействий $U_{l,\pi}$, которые, как правило, связаны или с распределением ресурсов $R_{l,\pi}$, доступных протоколу π_l , или с изменением параметров $\Omega_{l,\pi}$ алгоритмов $A_{l,\pi}$, на основе которых функционирует протокол.

Разные протоколы могут обеспечивать один и тот же показатель качества ($q_{l,\pi1} \cap q_{l,\pi2} \neq \emptyset$). Более того, как правило, в системе связи на одном уровне функционирования могут организовываться каскадные схемы протоколов, нацеленных на последовательное улучшение одного и того же показателя качества.

В качестве такого примера может выступать показатель качества – достоверность приема сигнала, для обеспечения которого последовательно применяются – протокол приема антенной системы, протокол помехоустойчивого приема, протокол фильтрации помех (рис. 3):

$$f_{\pi1}: \langle t, s_{\pi}, X_{l,\pi1}, U_{l,\pi1}, A_{\pi1} \rangle \rightarrow q_{l,\text{доcm1}}, q_{l,\text{доcm1}} \in q_{l,\pi1} \subseteq Q_l,$$

$$\gamma_{\pi1}: \langle t, s_{\pi}, X_{l,\pi1}, U_{l,\pi1}, A_{\pi1} \rangle \rightarrow Y_{l,\pi1};$$

$$f_{\pi2}: \langle t, s_{\pi}, Y_{l,\pi1}, U_{l,\pi2}, A_{\pi2} \rangle \rightarrow q_{l,\text{доcm2}}, q_{l,\text{доcm2}} \in q_{l,\pi2} \subseteq Q_l,$$

$$\text{при этом } q_{l,\text{доcm2}} > q_{l,\text{доcm1}},$$

$$\gamma_{\pi2}: \langle t, s_{\pi}, Y_{l,\pi1}, U_{l,\pi2}, A_{\pi2} \rangle \rightarrow Y_{l,\pi2};$$

$$f_{\pi3}: \langle t, s_{\pi}, Y_{l,\pi2}, U_{l,\pi3}, A_{\pi3} \rangle \rightarrow q_{l,\text{доcm3}}, q_{l,\text{доcm3}} \in q_{l,\pi3} \subseteq Q_l,$$

$$\text{при этом } q_{l,\text{доcm3}} > q_{l,\text{доcm2}},$$

$$\gamma_{\pi3}: \langle t, s_{\pi}, Y_{l,\pi2}, U_{l,\pi3}, A_{\pi3} \rangle \rightarrow Y_{l,\pi3}.$$

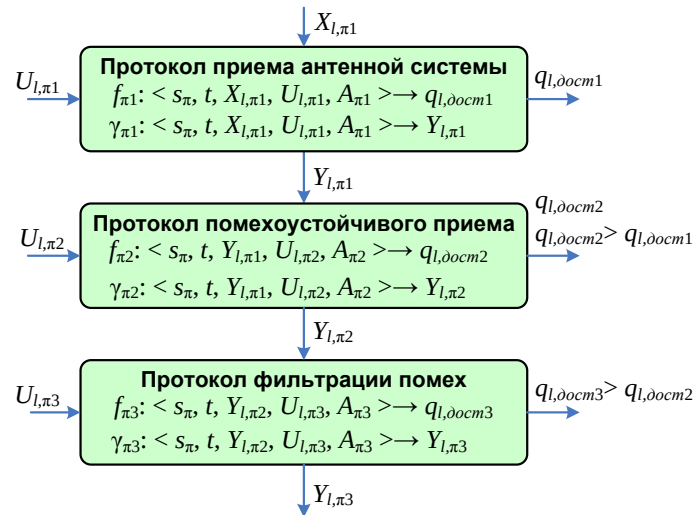


Рис. 3. Пример каскадной схемы протоколов функционирующих на одном уровне

Канал наблюдения $N_{l,\pi}$ протокола π_l со стороны системы управления связью обеспечивает сбор сведений о состоянии протокола s_π за счет наблюдения всех или части выходных параметров $Y_{l,\pi}$ и показателей QoS $Q_{l,\pi}$, которые обеспечиваются протоколом π_l . Целью наблюдения является определение состояния s_π протокола π_l и принятие решений о выработке управляющих воздействий $U_{l,\pi}$ на протокол. С учетом этого, наблюдение $N_{l,\pi}$ представляется вектором, составляющие которого являются соответственно наблюдениями элементов множеств $Y_{l,\pi}$ и $Q_{l,\pi}$. Данные компоненты образуют множество наблюдаемых параметров:

$$N_{l,\pi} = \langle Y_{l,\pi,N} \times Q_{l,\pi,N} \rangle, \quad (8)$$

где $Y_{l,\pi,N} \subseteq Y_{l,\pi}$ и $Q_{l,\pi,N} \subseteq Q_{l,\pi}$ – компоненты множеств $Y_{l,\pi}$ и $Q_{l,\pi}$ наблюдаемые системой управления связью.

Определение текущего состояния протокола s_π в условиях параметрического сужения $s_\pi \rightarrow \langle \{q_{l,\pi}\}, \{y_{l,\pi}\} \rangle \rightarrow \langle \{q_{l,\pi,N}\}, \{y_{l,\pi,N}\} \rangle \rightarrow N_{l,\pi}$, и сужения реакции, связанное с ограничением на время наблюдения $0 \leq T \leq t_{\text{набл}}$, в выражении (8) является предметом приложения теории наблюдения динамических систем [101, 102, 107] к исследованию систем управления связью и рассмотрено в работе [25]. Как показано в этой работе основными особенностями наблюдения протоколов в системе связи являются:

- дискретность процесса наблюдения: $T_\eta = \langle t_1, t_2, \dots, t_n, \dots \rangle$ в течении времени $t_{\text{набл}}$;
- временные задержки процессов сбора сведений о значениях компонент множеств $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$;
- потери сведений об отдельных наблюдениях $\eta_{l,\pi} \in N_{l,\pi}$ в процессе передачи по сети связи;
- ситуации нарушения порядка следования результатов наблюдения (в сети связи возможны ситуации, когда информация более позднего наблюдения $N_{l,\pi}(t_2)$ поступает раньше, чем информация предыдущего наблюдения $N_{l,\pi}(t_1)$, $t_2 > t_1$);

- наблюдение группы протоколов Π_l^* l -го уровня по их общим показателям качества Q_l^* и выходным параметрам Y_l^* , являющихся общими для всей группы:

$$\left\{ \begin{aligned} \Pi_l^* &= \bigcup \left(\pi_l \left| \left(\bigcap_{\pi_l} Q_{l,\pi} = Q_l^* \neq \emptyset \right) \wedge \left(\bigcap_{\pi_l} Y_{l,\pi} = Y_l^* \neq \emptyset \right) \right. \right) \\ N_{l,\Pi_l^*} &= \langle Q_l^* \times Y_l^* \rangle = \left(\bigcap_{\forall \pi_l \in \Pi_l^*} q_{l,\pi} \right) \cup \left(\bigcap_{\forall \pi_l \in \Pi_l^*} Y_{l,\pi} \right) \end{aligned} \right\},$$

что существенно затрудняет идентификацию состояния s_π каждого из протоколов π_l , входящих в группу Π_l^* ;

- наличие преднамеренных дестабилизирующих воздействий $V_{l,\pi}$, связанных с нарушением функционирования канала наблюдения ($N_{l,\pi}=0$) или подменой сведений о наблюдаемых показателях, входящих в множества $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$.

С учетом данных особенностей наблюдение $N_{l,\pi}$ протокола π_l можно отнести к одному из двух видов наблюдения [102]:

- 1) *наблюдаемость по направлению*, связанная с оценкой траектории изменения показателей, входящих в множества $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$ во времени:

$$\left[\begin{aligned} \eta_{l,\pi} &= \frac{d\{q_{l,\pi,N}\}}{dt} \\ \eta_{l,\pi} &= \frac{d\{y_{l,\pi,N}\}}{dt} \end{aligned} \right], \text{ где } \eta_{l,\pi} \in N_{l,\pi};$$

- 2) *локальная наблюдаемость*, связанная с фиксацией события $\eta_{l,\pi} \in N_{l,\pi}$, состоящего в изменении значения одного или нескольких наблюдаемых показателей $q_{l,\pi,N} \in N_{l,\pi}$ или $y_{l,\pi,N} \in N_{l,\pi}$ ниже некоторых граничных значений $q_{l,\pi}^{\text{треб}}$, $y_{l,\pi}^{\text{треб}}$:

$$\eta_{l,\pi} = \begin{cases} q_{l,\pi,\eta}^*, \text{ если } \exists \{q_{l,\pi,\eta}^* | q_{l,\pi,\eta}^* < q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi,N} \\ y_{l,\pi,\eta}^*, \text{ если } \exists \{y_{l,\pi,\eta}^* | y_{l,\pi,\eta}^* < y_{l,\pi}^{\text{треб}}\} \in Y_{l,\pi,N} \\ 0, \text{ если } \forall \left(\{q_{l,\pi,\eta} | q_{l,\pi,\eta} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi,N} \right) \wedge \left(\{y_{l,\pi,\eta} | y_{l,\pi,\eta} \geq y_{l,\pi}^{\text{треб}}\} \in Y_{l,\pi,N} \right) \end{cases}.$$

Канал $U_{l,\pi}$ управления протоколом π_l со стороны системы управления связью. Система управления связью по наблюдению $N_{l,\pi}$ вырабатывает функционал, задающий множество управляющих воздействий $U_{l,\pi}$, которые по каналу управления воздействует на протокол π_l . С учетом конечности множества состояний S_π и последовательности моментов $T_U = \langle t_1, t_2, \dots, t_n, \dots \rangle$ принятия решений по выдаче управляющих воздействий $U_{l,\pi} = \langle U_{l,\pi}(t_1), U_{l,\pi}(t_2), \dots, U_{l,\pi}(t_n), \dots \rangle$ такое управление $U_{l,\pi}$ можно назвать *программой управления*. Программа управления при любом начальном состоянии протокола $s_\pi(t_0)$ и наличии преднамеренных дестабилизирующих

воздействий $V_{l,\pi}$ должна обеспечивать выполнение критерия (7), т.е. существование предела (первое уравнение системы)

$$\begin{cases} Q_{l,\pi} = \lim_{\substack{t \rightarrow \infty \\ U_{l,\pi}(t)}} f_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}) \\ \forall \{q_{l,\pi} \geq q_{l,\pi}^{тр\epsilonб}\} \in Q_{l,\pi} \\ X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle \\ U_{l,\pi} = \langle u_{l,\pi} \times T_U \rangle \end{cases}.$$

Необходимо отметить, что ввиду особенностей наблюдения $N_{l,\pi}$ системы связи, изложенных выше, в контуре управления всегда присутствует неопределенность в определении текущего состояния протокола s_π . Еще одной чертой, характерной для протокола π_l , как для динамической системы, является наличие множества дестабилизирующих воздействий $V_{l,\pi}$. Эти аспекты позволяют отнести задачу разработки программы управления системой связи к задачам синтеза адаптивной робастной системы управления.

Наличие программы управления $U_{l,\pi}$ должно предусматривать план управления $U_{l,\pi}^{план} = \langle U_{l,\pi}(t_{тек+1}), U_{l,\pi}(t_{тек+2}), \dots, U_{l,\pi}(t_{тек+n}), \dots \rangle$ по обеспечению достижения выполнения критерия

$$\forall \{q_{l,\pi} \geq q_{l,\pi}^{тр\epsilonб}\} \in Q_{l,\pi}$$

за счетное число шагов n в будущие моменты времени. На план управления накладываются ограничения, что управление $U_{l,\pi}^{план}$ должно переводить протокол π_l в состояние s_π , которое является допустимым для этого протокола:

$$\begin{cases} s_\pi \in S_{l,\pi} \\ s_\pi = \Psi_{l,\pi}(t_0, t_{тек+n}, s_\pi(t_0), S_{l,\pi}, X_{l,\pi}, U_{l,\pi}^{план}, A_{l,\pi}) \\ X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle \\ U_{l,\pi}^{план} = \langle u_{l,\pi} \times T_U \rangle \end{cases}.$$

План управления должен предусматривать формирование управляющих воздействий $U_{l,\pi}^{план}$ в зависимости от текущего наблюдения $N_{l,\pi}(t_{тек})$, и подчиняться определенной стратегии управления, связанной с реализацией цели управления $\forall \{q_{l,\pi} \geq q_{l,\pi}^{тр\epsilonб}\} \in Q_{l,\pi}$. Как правило, для системы связи можно рассмотреть две основные стратегии управления при допущении о том, что принятие решения по выработке управления $U_{l,\pi}^{план}(t_{тек+1})$ осуществляется на каждом шаге независимо от предыдущих управлений и основано на результатах текущего наблюдения $N_{l,\pi}(t_{тек})$ [25]:

- 1) *вероятностная стратегия*, когда в условиях текущего наблюдения $N_{l,\pi}(t_{тек})$ в следующий момент времени осуществляется выбор такого управляющего воздействия $U_{l,\pi}^{план}(t_{тек+1})$ из имеющегося множества альтернатив $\{U_{l,\pi}(t_{тек+1})\}$, которое с наибольшей вероятностью ведет к выполнению выбранного критерия эффективности $q_{l,\pi} \geq q_{l,\pi}^{тр\epsilonб}$ ($q_{l,\pi} \in Q_{l,\pi}$):

$$U_{l,\pi}^{план} \prec \frac{\{U_{l,\pi}^{план}(t_{тек+1})\}}{N_{l,\pi}(t_{тек})} \rightarrow U_{l,\pi}(t_{тек+1}) \Big| P(q_{l,\pi}(t_{тек+1}) \geq q_{l,\pi}^{тр\epsilonб}) \rightarrow \max; \quad (9)$$

- 2) стратегия максимального приближения, когда в условиях текущего наблюдения $N_{l,\pi}(t_{\text{тек}})$ осуществляется выбор такого управляющего воздействия $U_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$, которое минимизирует отклонение выбранного показателя $q_{l,\pi}$ ($q_{l,\pi} \in Q_{l,\pi}$) от его требуемого значения $q_{l,\pi}^{\text{треб}}$:

$$U_{l,\pi}^{\text{план}} := \frac{\{U_{l,\pi}^{\text{план}}(t_{\text{тек}+1})\}}{N_{l,\pi}(t_{\text{тек}})} \rightarrow U_{l,\pi}(t_{\text{тек}+1}) \left(|q_{l,\pi}(t_{\text{тек}+1}) - q_{l,\pi}^{\text{треб}}| \rightarrow \min. \quad (10)$$

План управления при вероятностной стратегии может быть формализован на основе теории марковских и полумарковских процессов, а задача управления протоколом π_l может быть сведена к оптимизации семейства вероятностей вида (9). План управления при стратегии максимального приближения может быть формализован на основе теории адаптивного управления, при этом, задача управления протоколом π_l может быть сведена к оптимизации траектории воздействий минимизирующих последовательность шагов на каждом из которых реализуется управление (10).

Конкретизация плана управления $U_{l,\pi}^{\text{план}}$ может состоять в выделении отдельных объектов управления для протокола π_l , управление которыми планируется на очередном шаге $t_{\text{тек}+1}$. В зависимости от объекта управления по отношению к произвольному протоколу l -го уровня можно выделить:

- 1) самонастраивающиеся управления:

- управление ресурсами $R_{l,\pi}$, выделяемыми протоколу π_l из общего пула ресурсов l -го уровня

$$U_{l,\pi}: R_l \rightarrow \{R_{l,\pi}\};$$

- управление параметрами $\Omega_{l,\pi,a}$ отдельных алгоритмов $a \in A_{l,\pi}$

$$U_{l,\pi}: \{\Omega_{l,\pi}\} \rightarrow \arg A_{l,\pi}.$$

- 2) самоорганизующиеся управления:

- управление алгоритмами $A_{l,\pi}$ используемыми протоколом π_l из совокупности математического обеспечения $\{A_{l,\pi}\}$ и последовательностью их выполнения $\Theta_{l,\pi}$

$$U_{l,\pi}: \langle \{A_{l,\pi}\}, \{\Theta_{l,\pi}\} \rangle \rightarrow \langle A_{l,\pi}, \Theta_{l,\pi} \rangle;$$

- управление структурой функционального взаимодействия протоколов Π_l между собой на одном и том же уровне функционирования системы связи (отображение множества выходов $Y_{l,\pi}$ одних протоколов на множество входов $X_{l,\pi}$ других)

$$U_l: \langle \{\Theta_l\} \rangle \rightarrow \Theta_l, \text{ где } \Theta_l = \langle X_l, Y_l \rangle.$$

Ввиду ограниченности ресурсов R_l конкретного уровня задача их распределения между протоколами Π_l формализуется на основе теории комбинаторной оптимизации и, как правило, формулируется в виде задачи о ранце, или в виде задачи оптимизации расписания [108, 109]. Задачи выбора алгоритмов $A_{l,\pi}$ и их параметров $\{\Omega_{l,\pi,a}\}$, как правило, решается на основе методов линейного или динамического программирования с целью оптимизации выбранных показателей QoS: $\{q_{l,\pi} \rightarrow \max \mid q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\}$, $q_{l,\pi} \in Q_{l,\pi}$. Ввиду множественности показателей, входящих в $Q_{l,\pi}$, для перехода от множества локальных экстремумов $\{q_{l,\pi} \rightarrow \max\}$ к глобальному максимуму по интегральному показателю $\Sigma\{q_{l,\pi}\} \rightarrow \max$, как правило, вводят дополнительные

весовые коэффициенты для отдельных показателей $\{q_l\}$ и применяют метод многокритериальной оптимизации по Парето [110].

Управление $U_{l,\pi}$ в общем случае должно соответствовать принципу компенсации из теории управления по отношению к дестабилизирующим воздействиям $V_{l,\pi}$ и условиям естественной среды $\chi_{l,\pi}$. При этом компенсация может быть:

- *активной*, за счет выдачи управляющих воздействий $U_{l,\pi}$ на соответствующие объекты управления (см. выше);
- *пассивной*, за счет внесения некоторой избыточности (количественной, функциональной или временной) в математическое обеспечение $A_{l,\pi}$, в параметры $\Omega_{l,\pi}$ протокола π_l , в структуру взаимодействия протоколов Θ_l , а также в распределяемый протоколу ресурс $R_{l,\pi}$. Это позволит обеспечить выполнение требований по QoS $\forall \{q_{l,\pi} \geq q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}$ в более широком диапазоне параметров среды $X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle$.

Управляющие воздействия $U_{l,\pi}$ поступают по каналу управления, который представляет собой канал связи в составе сети связи или в отдельной управляющей сети. Это, а также общая специфика функционирования системы связи формирует основные особенности процесса управления протоколами в ней:

- дискретность процесса управления: $T_U = \langle t_1, t_2, \dots, t_n, \dots \rangle$;
- временные задержки в выдаче управляющих воздействий $U_{l,\pi}$;
- потери сообщений об управляющих воздействиях $U_{l,\pi}$ в процессе передачи по сети связи;
- ситуации нарушения причинности процесса управления (в пакетной сети связи возможны ситуации, когда более позднее управление $U_{l,\pi}(t_2)$ поступает раньше, чем сообщение о предыдущем управлении $U_{l,\pi}(t_1)$, $t_2 > t_1$);
- наличие дестабилизирующих воздействий $V_{l,\pi}$, связанных с нарушением функционирования канала управления ($u_{l,\pi} = 0$, $u_{l,\pi} \in U_{l,\pi}$) или подменой сообщений управляющих воздействий ($u_{l,\pi} = v_{l,\pi}$, где $u_{l,\pi} \in U_{l,\pi}$, $v_{l,\pi} \in V_{l,\pi}$).

Канал наблюдения $M_{l,\pi}$ протокола π со стороны системы дестабилизирующих воздействий. Канал наблюдения $M_{l,\pi}$ со стороны противника функционирует аналогично каналу наблюдения $N_{l,\pi}$ со стороны системы управления связью:

$$M_{l,\pi} = \langle Y_{l,\pi,M} \times Q_{l,\pi,M} \rangle,$$

где $Y_{l,\pi,M} \subseteq Y_{l,\pi}$ и $Q_{l,\pi,M} \subseteq Q_{l,\pi}$ – элементы множеств $Y_{l,\pi}$ и $Q_{l,\pi}$ наблюдаемые системой управления воздействиями противника.

Вместе с тем каналу наблюдения $M_{l,\pi}$ свойственна одна принципиальная особенность. Ввиду того, что возможности наблюдения противника $M_{l,\pi}$ ниже возможностей канала наблюдения системы связи $N_{l,\pi}$, то противник не может получить доступ ко всем наблюдаемым параметрам $Y_{l,\pi,N}$ и $Q_{l,\pi,N}$ вектора $N_{l,\pi}$. Таким образом, количество параметров протокола π_l , наблюдаемых

противником по каналу $M_{l,\pi}$, как правило, меньше, чем количество параметров $N_{l,\pi}$, наблюдаемых системой управления связью, т.е.

$$M_{l,\pi} \subseteq N_{l,\pi} \subseteq \langle Y_{l,\pi} \times Q_{l,\pi} \rangle, \quad (11)$$

при этом равенство $M_{l,\pi} = N_{l,\pi}$ обеспечивается только в случаях, когда система наблюдения противника получила полный доступ к каналу наблюдения системы управления связью (например, путем перехвата сообщений канала наблюдения $N_{l,\pi}$).

Целью наблюдения $M_{l,\pi}$ является определение текущего состояния протокола s_π и принятие решений о выработке преднамеренных воздействий $V_{l,\pi}$ на протокол π_l . С учетом выражения (11) можно сделать вывод о том, что система воздействия всегда наблюдает протокол π_l с меньшей степенью достоверности, чем система управления связью.

При наблюдении системы связи противником на первом этапе необходимо решить задачу идентификации множества конкретных протоколов $\{\pi_l\}$, используемых на l -ом уровне среди множества протоколов Π_l по наблюдению $M_{l,\pi}$. Как правило, данная задача решается на основе теории идентификации и теории классификации. На втором этапе решается задача определения состояния s_π для каждого конкретного протокола π_l . Как правило, обе задачи решаются за счет формирования признакового пространства и построения в нем траекторий наблюдения показателей $\{\mu_{l,\pi}(t)\} \in M_{l,\pi}$ в течении некоторого времени $t_{\text{набл}}$, достаточным для накопления данных и идентификации конкретных протоколов $\{\pi_l\} \in \Pi_l$ и их состояний $\{s_\pi\}$.

Основными проблемными аспектами, связанными с каналом наблюдения протокола со стороны противника, являются:

- наличие временной задержки связанной с накоплением данных наблюдения в течении $t_{\text{набл}}$;
- наблюдение группы протоколов Π_l^* l -го уровня по их общим показателям качества Q_l^* и выходным параметрам Y_l^* , являющимися общими для всей группы:

$$\left\{ \begin{aligned} \Pi_l^* &= \bigcup \left(\pi_l \left| \left(\bigcap_{\Pi_l} Q_{l,\pi,M} = Q_{l,M}^* \neq \emptyset \right) \wedge \left(\bigcap_{\Pi_l} Y_{l,\pi,M} = Y_{l,M}^* \neq \emptyset \right) \right. \right) \\ M_{l,\Pi_l^*} &= \langle Q_{l,M}^* \times Y_{l,M}^* \rangle = \left(\bigcap_{\forall \pi_l \in \Pi_l^*} Q_{l,\pi,M} \right) \cup \left(\bigcap_{\forall \pi_l \in \Pi_l^*} Y_{l,\pi,M} \right) \end{aligned} \right\},$$

что существенно затрудняет идентификацию состояния s_π каждого из протоколов $\pi_l \in \Pi_l^*$, входящих в группу;

- сложность достоверного определения состояния протокола s_π в условиях параметрического сужения:

$$\{s_\pi\} \rightarrow \{\pi_l\} \rightarrow \Pi_l \rightarrow \langle Y_l \times Q_l \rangle \rightarrow \langle Y_{l,M} \times Q_{l,M} \rangle \rightarrow M_l \rightarrow \{M_{l,\pi}\},$$

и сужения реакции, связанное с ограничениями на дискретность $T_\mu = \langle t_1, t_2, \dots, t_n, \dots \rangle$ и общую длительность времени наблюдения $t_{\text{набл}}$;

- возможности системы связи по активному противодействию каналу наблюдения противника, за счет выполнения мероприятий по противодействию средствам разведки ($\mu_{l,\pi} = 0$), а также создания ложных систем и средств связи, реализующих внедрение в канал

наблюдения противника $M_{l,\pi}$ дезинформации об истинных режимах работы и об используемых в системе связи протоколах;

- наличие требований по скрытности наблюдения.

Для повышения уровня достоверности наблюдения системой дестабилизирующих воздействий могут выдаваться тестовые воздействия $V_{l,\pi}^{\text{тест}}$, которые соответствуют однозначно идентифицируемой траектории изменения параметров $Q_{l,\pi,M}(t)$ и $Y_{l,\pi,M}(t)$, наблюдаемых в канале $M_{l,\pi}$. Бескомпроматное использование таких тестовых воздействий $V_{l,\pi}^{\text{тест}}$, подобранных для идентификации протоколов π_l , а также их состояний $\{s_\pi\}$ на начальном этапе конфликта позволит собрать сведения о составе и функциональной структуре l -го уровня, а на этапах развития конфликта – контролировать эффективность воздействия.

Канал воздействия $V_{l,\pi}$ на протокол π со стороны системы дестабилизирующих воздействий. По итогам наблюдения $M_{l,\pi}$ система дестабилизирующих воздействий принимает решение о выборе и осуществление воздействия $V_{l,\pi}=\{v_{l,\pi}\}$ из множества воздействий V_l , которые могут быть осуществлены на l -ом уровне функционирования. Выбор воздействия $V_{l,\pi}$ должен учитывать совокупность факторов естественной среды $\chi_{l,\pi}$, выделенный протоколу ресурс $R_{l,\pi}$, а также состав математического обеспечения $A_{l,\pi}$ и его параметры $\Omega_{l,\pi}$ протокола π_l . Фактически, совокупность протокола π_l и системы дестабилизирующих воздействий образуют как бы еще один контур управления с антагонистическим критерием достижения цели воздействия – снижения заданного или всех показателей качества протокола $q_{l,\pi}$ ниже требуемых значений $q_{l,\pi}^{\text{треб}}$:

$$\left[\begin{array}{l} \exists \{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi} \\ \forall \{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi} \end{array} \right]. \quad (12)$$

Конечное множество воздействий $V_{l,\pi}=\{v_{l,\pi}\}$ на интервале времени T_V образуют программу воздействий. Программа воздействий может реализоваться:

- в дискретном времени
 $V_{l,\pi}=\langle V_{l,\pi}(t_1), V_{l,\pi}(t_2), \dots, V_{l,\pi}(t_n), \dots \rangle, T_V=\langle t_1, t_2, \dots, t_n, \dots \rangle;$
- в непрерывном времени
 $V_{l,\pi}=V_{l,\pi}(t), t \in T_V.$

Программа воздействий $V_{l,\pi}$ при любом начальном состоянии протокола $s_\pi(t_0)$ и наличии управляющих воздействий $U_{l,\pi}$ должна обеспечивать выполнение критерия (12), т.е. существование предела

$$\left\{ \begin{array}{l} q_{l,\pi} = \lim_{\substack{t \rightarrow T_V \\ V_{l,\pi}(t)}} f_{l,\pi}(t, s_\pi, X_{l,\pi}, U_{l,\pi}, A_{l,\pi}) \\ \exists \{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi} \\ X_{l,\pi} = \langle R_{l,\pi} \times \chi_{l,\pi} \times V_{l,\pi} \rangle \\ U_{l,\pi} = \langle \{u_{l,\pi}\} \times T_U \rangle \end{array} \right. .$$

Наличие программы воздействия $V_{l,\pi}$ должно предусматривать план воздействия $V_{l,\pi}^{\text{план}}=\langle V_{l,\pi}(t_{\text{тек}}+1), V_{l,\pi}(t_{\text{тек}}+2), \dots, V_{l,\pi}(t_{\text{тек}}+n), \dots \rangle$ по обеспечению

достижения выполнения критерия $\exists \{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\} \in Q_{l,\pi}$ за счетное число шагов n , в будущие моменты времени.

План воздействия должен предусматривать формирование воздействий $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ в зависимости от текущего наблюдения $M_{l,\pi}(t_{\text{тек}})$, и подчиняться определенной стратегии, связанной с реализацией цели воздействия ($\exists \{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$). Как правило, применительно к системе воздействия на отдельный протокол π_l можно рассмотреть следующие основные стратегии, при допущении о том, что принятие решения по выработке воздействия $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ осуществляется на каждом шаге независимо от предыдущих воздействий и основано на результатах наблюдения $M_{l,\pi}(t_{\text{тек}})$:

- 1) *вероятностная стратегия*, когда при текущем наблюдении $M_{l,\pi}(t_{\text{тек}})$, в следующий момент времени осуществляется выбор такого воздействия $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$ из имеющегося множества альтернатив $\{V_{l,\pi}(t_{\text{тек}+1})\}$, которое с наибольшей вероятностью ведет к выполнению критерия эффективности воздействия (12) по одному или нескольким показателям $q_{l,\pi}$, входящим в множество $Q_{l,\pi,v} = \{q_{l,\pi} \mid q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$ ($Q_{l,\pi,v} \in Q_{l,\pi} \in Q_l$) т.е.

$$V_{l,\pi}^{\text{план}} := \frac{\{V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})\}}{M_{l,\pi}(t_{\text{тек}})} > \rightarrow V_{l,\pi}(t_{\text{тек}+1}) \mid P(q_{l,\pi}(t_{\text{тек}+1}) < q_{l,\pi}^{\text{треб}}) \rightarrow \max; \quad (13)$$

- 2) *стратегия максимального отклонения*, когда при текущем наблюдении $M_{l,\pi}(t_{\text{тек}})$ осуществляется выбор такого воздействия $V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})$, которое максимизировало бы отклонение показателей $q_{l,\pi} \in Q_{l,\pi,v}$ от их требуемых значений $q_{l,\pi}^{\text{треб}}$:

$$V_{l,\pi}^{\text{план}} := \frac{\{V_{l,\pi}^{\text{план}}(t_{\text{тек}+1})\}}{M_{l,\pi}(t_{\text{тек}})} > \rightarrow V_{l,\pi}(t_{\text{тек}+1}) \mid (q_{l,\pi}^{\text{треб}} - q_{l,\pi}(t_{\text{тек}+1})) \rightarrow \max. \quad (14)$$

Ввиду сложности организации воздействий $V_{l,\pi}$, ориентированных на конкретный протокол π_l , и с учетом их интегрального характера целесообразнее рассмотреть стратегии воздействий V_l , ориентированных на весь l -ый уровень функционирования. В этом случае стратегии (13) и (14) могут быть модифицированы с учетом максимизации числа поражаемых протоколов и уровней дестабилизирующих эффектов в каждом из них:

- 3) *вероятностная стратегия максимизации количества пораженных протоколов*, когда при текущем наблюдении $M_l(t_{\text{тек}})$ осуществляется выбор такого воздействия $V_l^{\text{план}}(t_{\text{тек}+1})$ из имеющегося множества альтернатив $\{V_l(t_{\text{тек}+1})\}$, которое с наибольшей вероятностью ведет к выполнению критерия эффективности воздействия $\{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$ по выбранным показателям $q_{l,\pi}$, входящим в множество $Q_{l,v} = \bigcup Q_{l,\pi,v}$, в максимальном числе протоколов $\Pi_{l,v}$ из множества Π_l

$$V_l^{\text{план}} := \frac{\{V_l^{\text{план}}(t_{\text{тек}+1})\}}{M_l(t_{\text{тек}})} > \rightarrow V_l(t_{\text{тек}+1}) \mid \begin{cases} |\Pi_{l,v}| \rightarrow \max \\ P(|\Pi_{l,v}|) \rightarrow \max \end{cases}, \quad (15)$$

где $|\Pi_{l,v}|$ - число элементов множества протоколов Π_l , поражаемых воздействием V_l ;

4) стратегия максимального интегрального отклонения, когда при наблюдении $M_l(t_{\text{тек}})$ осуществляется выбор такого воздействия $V_l^{\text{план}}(t_{\text{тек}+1})$, которое максимизировало отклонение показателей $q_{l,\pi} \in Q_{l,v}$ от их требуемых значений $q_{l,\pi}^{\text{треб}}$ в максимальном числе протоколов $\Pi_{l,v}$ из множества Π_l :

$$V_l^{\text{план}} :< \frac{\{V_l^{\text{план}}(t_{\text{тек}+1})\}}{M_l(t_{\text{тек}})} > \rightarrow V_l(t_{\text{тек}+1}) \left\| \begin{array}{l} |\Pi_{l,v}| \rightarrow \max \\ \sum_{\pi \in \Pi_{l,v}} (q_{l,\pi}^{\text{треб}} - q_{l,\pi}(t_{i+1})) \rightarrow \max \end{array} \right. \quad (16)$$

В случае наличия единственного показателя качества $|Q_{l,\pi,v}|=1$, по которому оценивается эффективность воздействия $V_{l,\pi}$ (или V_l). Выражения (13)-(16) будут напрямую определять стратегию очередного шага в плане $V_{l,\pi}^{\text{план}}$ (или в $V_l^{\text{план}}$). Если в множество $Q_{l,\pi,v}$ входит несколько показателей качества ($|Q_{l,\pi,v}|>1$), то для перехода от множества локальных экстремумов к глобальному максимуму по интегральному показателю необходимо ввести дополнительные весовые коэффициенты для отдельных показателей $q_{l,\pi} \in Q_{l,v}$ и использовать метод многокритериальной оптимизации по Парето [110].

Анализ отличительных особенностей стратегий (13, 14) и (15, 16) позволяет сделать следующий вывод. Использование стратегий (13, 14), а также воздействий, ориентированных на подавление отдельных протоколов π_l , целесообразно, в случае высокой степени наблюдаемости $M_{l,\pi}$, когда возможно параметрическое выделение состояния s_π каждого из протоколов π_l множества Π_l

$$M_l \rightarrow M_{l,\pi} \rightarrow <Y_{l,\pi,M} \times Q_{l,\pi,M}> \rightarrow \{\pi_l\} \rightarrow \{s_\pi\}.$$

Стратегии (15, 16) и воздействия V_l , обладающие максимальным «площадным» эффектом $|\Pi_{l,v}| \rightarrow \max$, целесообразно использовать, когда по наблюдению M_l сложно осуществить параметрическое выделение состояния s_π каждого из протоколов π_l , а возможно только определение общего направления функционирования множества протоколов Π_l

$$M_l \rightarrow <Y_{l,M} \times Q_{l,M}> \rightarrow \Pi_l.$$

План воздействий $V_{l,\pi}^{\text{план}}$ при вероятностных стратегиях (13, 15) может быть формализован на основе теории марковских и полумарковских процессов, а задача управления воздействием на протокол π_l или на их множество Π_l может быть сведена к оптимизации семейства вероятностей вида (13). План воздействий $V_{l,\pi}^{\text{план}}$ и $V_l^{\text{план}}$ при стратегиях (14, 16) основанных на максимальном отклонении может быть формализован на основе теории адаптивного управления при этом задача воздействия на протокол π_l или на их множество Π_l может быть сведена к оптимизации траектории воздействий $V_l(t_{\text{тек}+1})$, $V_l(t_{\text{тек}+2})$, ..., $V_{l,\pi}(t_{\text{тек}+n})$, минимизирующих число шагов n , на каждом из которых реализуется управление (14) или (16), для достижения условия (12).

В работах [3, 20, 25] вводится понятие «ресурса воздействия» $R_v = \{r_{l,v}\}$ как совокупности временных, энергетических и вероятностных параметров, описывающих одно или несколько воздействий V_l , с целью дестабилизирующего влияния на элементы системы связи. В тех же работах показано, что система воздействий должна минимизировать расход своего

ресурса при одновременном рациональном его распределении между отдельными воздействиями $\{V_{l,\pi}\}$. С учетом вышеуказанного целесообразно дополнить стратегии (13-16) дополнительным критерием выбора воздействий – по итогам наблюдения $M_l(t_{\text{тек}})$ на следующем шаге $t_{\text{тек}+1}$ целесообразно выбирать такое воздействие $V_l(t_{\text{тек}+1})$, которое минимизирует суммарный расход ресурса воздействия $R_{l,v}$ на l -ом уровне функционирования

$$V_l^{\text{план}} :< \frac{\{V_l^{\text{план}}(t_{\text{тек}+1})\}}{M_l(t_{\text{тек}})} > \rightarrow V_l(t_{\text{тек}+1})|R_{l,v} \rightarrow \min, \quad (17)$$

при этом возможно выделить отдельную подзадачу рационального распределения общего ресурса $R_{l,v}$ по отдельным ресурсам $\{R_{l,\pi,v}\}$, выделяемым каждому воздействию $V_{l,\pi}$ на отдельные протоколы $\{\pi_l\}$, с целью реализации стратегий (13-16) и выполнения критерия $R_{l,v} \rightarrow \min$.

Конкретизация плана воздействия $V_{l,\pi}^{\text{план}}$ будет состоять в выделении отдельных объектов, воздействие на которые планируется на очередном шаге $t_{\text{тек}+1}$. В зависимости от объекта воздействия по отношению к произвольному протоколу l -го уровня можно выделить:

1) воздействия на входные данные:

- ограничение как общего ресурса l -го уровня R_l , так и ресурсов отдельных протоколов $R_{l,\pi}$

$$V_l: R_l \rightarrow R_{l,v} \mid \exists \{R_{l,v} < R_l\},$$

$$V_{l,\pi}: R_{l,\pi} \rightarrow R_{l,\pi,v} \mid \exists \{R_{l,\pi,v} < R_{l,\pi}\};$$

- усугубление дестабилизирующих факторов естественной среды $\chi_{l,\pi}$ функционирования протокола π_l

$$V_{l,\pi}: (X_{l,\pi} = < R_{l,\pi} \times \chi_{l,\pi} >) \rightarrow (X_{l,\pi} = < R_{l,\pi} \times (\chi_{l,\pi} \times V_{l,\pi}) >);$$

- ограничение или подмена входных параметров $X_{l,\pi}$ протокола

$$V_{l,\pi}: X_{l,\pi} \rightarrow X_{l,\pi,v} \mid \exists \{x_{l,\pi,v} = 0\}, \text{ при условии } |X_{l,\pi}| = |X_{l,\pi,v}|,$$

$$V_{l,\pi}: X_{l,\pi} \rightarrow X_{l,\pi,v} \mid \exists \{x_{l,\pi} = v_{l,\pi}\}, \text{ при условии } |X_{l,\pi}| = |X_{l,\pi,v}|.$$

2) воздействия на функционал протокола:

- функциональная блокировка за счет ограничения параметров $\omega \in \Omega_{l,\pi}$ в математическом обеспечении $A_{l,\pi}$ протокола π_l

$$V_{l,\pi}: \Omega_{l,\pi} \rightarrow \Omega_{l,\pi,v} \mid \exists \{\omega = 0 \mid \omega \in \Omega_{l,\pi,v}\}, \text{ при } |\Omega_{l,\pi}| = |\Omega_{l,\pi,v}|;$$

- функциональная блокировка за счет ограничения исполнения алгоритмов $A_{l,\pi}$ в математическом обеспечении протокола π_l

$$V_{l,\pi}: A_{l,\pi} \rightarrow A_{l,\pi,v} \mid \exists \{a = \emptyset \mid a \in A_{l,\pi,v}\}, \text{ при } |A_{l,\pi}| = |A_{l,\pi,v}|;$$

- функциональная блокировка за счет ограничения функциональных связей $\Theta_{l,\pi}$ алгоритмов $A_{l,\pi}$ в протоколе π_l

$$V_{l,\pi}: \langle A_{l,\pi}, \Theta_{l,\pi} \rangle \rightarrow \Theta_{l,\pi,v} \mid \exists \{\theta = \emptyset \mid \theta \in \Theta_{l,\pi,v}\} \wedge \{\theta \neq \emptyset \mid \theta \in \Theta_{l,\pi}\}_i = 1,$$

где $\wedge$ - знак конъюнкции (логическое «и»), $\theta \in \Theta_{l,\pi}$;

- навязывание ложной логики работы за счет подмены или искажения параметров алгоритмов $\Omega_{l,\pi}$ в математическом обеспечении $A_{l,\pi}$ протокола π_l

$$V_{l,\pi}: \Omega_{l,\pi} \rightarrow \Omega_{l,\pi,v} \mid \exists \{\omega = v_{l,\pi,a} \mid \omega \in \Omega_{l,\pi,v}\}, \text{ при } |\Omega_{l,\pi}| = |\Omega_{l,\pi,v}|;$$

- навязывание ложной логики за счет подмены или искажения отдельных алгоритмов a в математическом обеспечении $A_{l,\pi}$ протокола π_l

$$V_{l,\pi}: A_{l,\pi} \rightarrow A_{l,\pi,v} \mid \exists \{a=v_{l,\pi,a} \mid a \in A_{l,\pi,v}\}, \text{ при } |A_{l,\pi}| = |A_{l,\pi,v}|;$$
- навязывание ложной логики, за счет нарушения функциональных связей $\Theta_{l,\pi}$ алгоритмов $A_{l,\pi}$ в математическом обеспечении протокола π_l

$$V_{l,\pi}: \langle A_{l,\pi}, \Theta_{l,\pi} \rangle \rightarrow \Theta_{l,\pi,v} \mid \exists (\{\theta=v_{l,\pi,\theta} \mid \theta \in \Theta_{l,\pi,v}\} \wedge \{\theta \neq \emptyset \mid \theta \in \Theta_{l,\pi}\})=1,$$

где $\theta \in \Theta_{l,\pi}$.

Как правило, воздействия, ориентированные на входные данные, реализуются внешними по отношению к протоколу средствами и способами (воздействие физических и радиоэлектронных средств подавления, подмена или искажение передаваемых по системе связи пакетов, DOS и DDOS атаки и т.д.). Воздействия, ориентированные на функциональную блокировку или навязывание ложной логики, требуют глубокого знания функционирования протокола и реализуются программными и аппаратными закладками, а также с помощью деструктивных программных средств (компьютерных вирусов).

Воздействие $V_{l,\pi}$ в общем случае должно соответствовать принципу компенсации из теории управления по отношению к управлению $U_{l,\pi}$ и условиям среды $\chi_{l,\pi}$. При этом такое компенсационное воздействие может быть:

- *активным* за счет непосредственных воздействий $V_{l,\pi}$ на соответствующие объекты (см. выше);
- *пассивным* за счет внесения в математическое обеспечение $A_{l,\pi}$ и параметры $\Omega_{l,\pi}$ протокола π_l , а также в структуру взаимодействия протоколов Θ_l специализированных «закладок». Их наличие позволит реализовать режимы снижения быстродействия, квази-случайных вычислительных ошибок, переход в ложные режимы функционирования, а также режимы «внутреннего благоприятствования» воздействиям $V_{l,\pi}$. Это обеспечит выполнение критерия эффективности воздействия $\exists \{q_{l,\pi} < q_{l,\pi}^{\text{треб}}\}$ в более широком диапазоне воздействий $V_{l,\pi}$ и для большего числа показателей $\{q_{l,\pi}\} \in Q_{l,\pi,v}$.

Специфика конфликтного взаимодействия с системой связи формирует основные особенности процесса воздействий на протоколы:

- управление выдачей воздействий $V_{l,\pi}$ и V_l ведется в условиях ограниченной наблюдаемости протоколов l -го уровня;
- стратегии воздействий $V_{l,\pi}$ и V_l , а также выбор конкретных способов воздействий на l -ом уровне зависит от степени наблюдаемости этого уровня;
- любые воздействия $V_{l,\pi}$ и V_l реализуют интегральный эффект поражения, так как протоколы взаимосвязаны при решении задач l -го уровня функционирования;
- воздействия $V_{l,\pi}$ и V_l на l -ом уровне могут быть ориентированны на входные параметры или на функционал протокола(ов) и при этом могут носить как пассивный, так и активный характер;

- воздействиям $V_{l,\pi}$ и V_l свойственна инертность реакции на наблюдение $M_{l,\pi}$.

Данные особенности процессов воздействия, а также особенности наблюдения $M_{l,\pi}$, изложенные выше, позволяют сделать вывод, что в контуре управления воздействиями всегда присутствует неопределенность определения состояний, как отдельных протоколов, так и их множества на l -ом уровне. Эти аспекты позволяют отнести задачу разработки системы воздействия к задачам робастного анализа с целью поиска неустойчивых режимов функционирования протокола системы связи как динамической системы.

Таким образом, любой протокол π_l может быть описан как динамическая система, функционирующая в сложной параметрической среде, при этом сам протокол фактически является частью двух контуров управления – системы управления связью и системы управления воздействиями с антагонистическими целями функционирования. Такая функциональная дуальность определяет информационный конфликт вышеуказанных систем управления, который происходит и развивается в приложении к конкретному протоколу. Дополнительно к вышеуказанному надо отметить, что протокол является частью сложной функционально-взаимосвязанной структуры как в горизонтальной области – в соответствии задачами отдельного уровня OSI, так и в вертикальной в области – в соответствии с задачами межуровневого протокольного взаимодействия. В связи с этим целесообразно на основе представленной модели протокола функционирующего на отдельном уровне OSI рассмотреть функционирование всей функционально-взаимосвязанной структуры системы связи с учетом ее многоуровневого иерархического конфликтного взаимодействия с системой дестабилизирующих воздействий.

Многоуровневая иерархическая динамическая модель системы связи

Особенность системы связи состоит в том, что она, в соответствии с моделью OSI, функционирует на семи иерархических уровнях. При этом на каждом из уровней имеется множество функционально связанных протоколов, решающих задачи связи данного уровня. Несмотря на то, что эталонная модель OSI постулирует независимость отдельных уровней и необходимость решения задач каждого уровня самостоятельно и независимо, на самом деле уровни OSI являются функционально вложенными «снизу-вверх». Таким образом, отказ на нижних уровнях ведет к изменению показателей качества связи на более высоких уровнях. В связи с этим целесообразно дополнить «принцип независимости уровней системы связи», рассматриваемый в модели OSI учетом функционально-иерархической вложенности нижестоящих уровней в вышестоящие, за счет использования методов теории сложных иерархических систем.

Каждый l -ый уровень системы связи решает свои функциональные задачи. При этом непосредственно сам уровень образован совокупностью функционально-взаимодействующих протоколов $\Pi_l = \cup \pi_l$, которые функционируют в параметрическом пространстве среды $X_l = R_l \times \chi_l \times V_l$ (где $\chi_l = \cup \chi_{l,\pi}$, $R_l = \cup R_{l,\pi}$, $V_l = \cup V_{l,\pi}$). В соответствии с этими особенностями каждому

уровню присущи специфические для него параметры естественной среды χ_l , ресурсы R_l и воздействия V_l , при этом эффективность функционирования нижних уровней напрямую определяет эффективность функционирования более верхних уровней.

Рассмотрим модель системы связи как обобщение модели протокола, рассмотренной выше (рис. 4).

Как показано на рис. 4 система связи состоит из 7 уровней, которые соответствуют модели OSI, и каждому из уровней соответствует собственная совокупность протоколов. С учетом формального описания протокола, представленного выше, каждый уровень модели в составе иерархической модели сети будет описываться следующими параметрами и отображениями.

1) Входные параметры l -ого уровня:

- множество обобщенных параметров среды $X_l = \langle R_l \times \chi_l \times V_l \rangle$ (где $\chi_l = \bigcup \chi_{l,\pi}$, $R_l = \bigcup R_{l,\pi}$, $V_l = \bigcup V_{l,\pi}$), в которой функционирует множество протоколов Π_l ($\Pi_l = \bigcup \pi_l$) на l -ом уровне, включающие в себя:
 - множество параметров естественной среды l -го уровня χ_l ($\chi_l \subseteq \chi$);
 - множество ресурсов связи l -го уровня R_l ($R_l \subseteq R$);
 - множество преднамеренных воздействий V_l реализуемых системой дестабилизирующих воздействий на l -ом уровне и влияющих на функционирование протоколов Π_l ($V_l \subseteq V$);
- множество управляющих воздействий $U_l = \langle \{U_{l,\pi}\} \times T \rangle$ ($U_l \subseteq U$) на протоколы Π_l со стороны системы управления связи на l -ом уровне;
- множество моментов времени функционирования системы связи T .

2) Отображения, определяющие общую динамическую модель l -ого уровня системы связи:

- множество алгоритмов A_l протоколов Π_l на l -ом уровне системы связи:

$$A_l = \bigcup_{\pi_l} A_{l,\pi}; \quad (18)$$

- множество параметров Ω_l алгоритмов A_l протоколов Π_l на l -ом уровне системы связи:

$$\Omega_l = \bigcup_{\pi_l} \Omega_{l,\pi}; \quad (19)$$

- отображение ψ_l , задающие смену состояний s_l l -ого уровня системы связи:

$$s_l = \{s_\pi\} \cup \Theta_l = \psi_l(t_0, t, \{\pi\}, \{S_\pi\}, X_l, U_l, A_l, \Theta_l), \quad (20)$$

при этом состояние l -ого уровня определяется как объединение множества состояний всех протоколов этого уровня $\{s_\pi\}$ и состояния функционально-структурных связей между протоколами Θ_l ;

- отображение f_l , определяющее выходные показатели качества обслуживания Q_l , которые обеспечивают протоколы Π_l на l -ом уровне функционирования:

$$Q_l = f_l(t, s_l, X_l, U_l, A_l); \quad (21)$$

- отображение γ_l , определяющее выходные параметры Y_l протоколов Π_l на l -ом уровне:

$$Y_l = \gamma_l(t, s_l, X_l, U_l, A_l); \quad (22)$$

- отображение φ_l , определяющее параметрическое множество среды X_{l+1} функционирования протоколов более высокого уровня Π_{l+1} :

$$X_{l+1} = \varphi_l(s_\pi, t, X_l, U_l, A_l). \quad (23)$$

3) Выходные параметры:

- множество выходных параметров l -ого уровня Y_l ;
- множество показателей качества обслуживания Q_l , которые обеспечиваются на l -ом уровне функционирования;
- множество параметров среды для функционирования протоколов более высокого уровня X_{l+1} ;
- канал наблюдения $N_l = \text{UN}_{l,\pi} = \langle Y_{l,N} \times Q_{l,N} \rangle$ со стороны системы управления связью в интересах принятия решений по управлению связью;
- канал наблюдения $M_l = \text{UN}_{l,\pi} = \langle Y_{l,M} \times Q_{l,M} \rangle$ со стороны системы дестабилизирующих воздействий в интересах принятия решений по целесообразному применению воздействий V_l .

С учетом вышеизложенного иерархическая модель системы связи как совокупности уровней модели OSI (рис. 4) будет определяться следующими параметрами и отображениями.

1) Входные параметры системы связи:

- множество обобщенных параметров среды $X = \cup X_l$, включающие в себя:
- множество параметров естественной среды $\chi = \cup \chi_l$;
- множество ресурсов связи $R = \cup R_l$;
- множество воздействий $V = \cup V_l$ реализуемых системой дестабилизирующих воздействий на l -ых уровнях функционирования;
- множество управляющих воздействий $U = \cup U_l$ со стороны систем управления связью на l -ых уровнях функционирования;
- множество моментов времени функционирования T .

2) Отображения, определяющие динамическую модель системы связи:

- множество алгоритмов A системы связи:

$$A = \cup A_l; \quad (24)$$

- множество параметров Ω алгоритмов A системы связи:

$$\Omega = \cup \Omega_l; \quad (25)$$

- множество протоколов Π системы связи:

$$\Pi = \cup \Pi_l; \quad (26)$$

- отображение ψ , задающие смену состояний S системы связи:
$$S = \{S_l\} \cup \Theta = \psi(t_0, t, \{S_l\}, X, U, A, Z, E, K, \Lambda, \Theta), \quad (27)$$
где: $Z = \{z_i\}$ – множество узлов системы связи; $E = \{e_i\}$ – множество средств связи, установленных на узлах; $K = \{k_{ij}\}$ – множество каналов связи, соединяющих узлы, при этом предполагается, что k_{ij} соединяет узлы z_i и z_j в случае если средства связи $e_i \in z_i$ и $e_j \in z_j$, размещенные на этих узлах используют один и тот же протокол связи $\pi_{i,k}$;
- множество отображений f , определяющих выходные показатели качества обслуживания Q системы связи:
$$Q = f(t, S, X, U, A), f = \cup f_i, Q = \cup Q_i; \quad (28)$$
- множество отображений γ , определяющих выходные параметры Y системы связи:
$$Y = \gamma(t, S, X, U, A), \gamma = \cup \gamma_i, Y = \cup Y_i; \quad (29)$$
- множество отображений φ , определяющих межуровневые связи между уровнями системы связи:
$$\varphi = \cup \varphi_i. \quad (30)$$

Фактически множество отображений φ определяет отличие данной модели от классической модели OSI, которая в явном виде не задает межуровневые отображения.

3) Выходные параметры:

- множество выходных параметров системы связи Y ;
- итоговые выходные параметры системы связи Y_7 ;
- множество показателей качества обслуживания Q системы связи;
- канал наблюдения $N = \cup N_i = \langle Y_N \times Q_N \rangle$ со стороны системы управления связью в интересах принятия решений по управлению связью;
- канал наблюдения $M = \cup M_i = \langle Y_M \times Q_M \rangle$ со стороны системы дестабилизирующих воздействий в интересах принятия решений по применению многоуровневых воздействий V .

Рассмотрим особенности функционирования системы связи более подробно. Основные особенности системы связи как динамической системы в аспектах ее функционирования, управления, наблюдения и конфликтного взаимодействия с системой дестабилизирующих воздействий могут быть рассмотрены по аналогии с вышерассмотренной моделью отдельного протокола. В связи с этим при моделировании системы связи акцентируем внимание на основных эмерджентных свойствах с учетом ее многоуровневого иерархического построения.

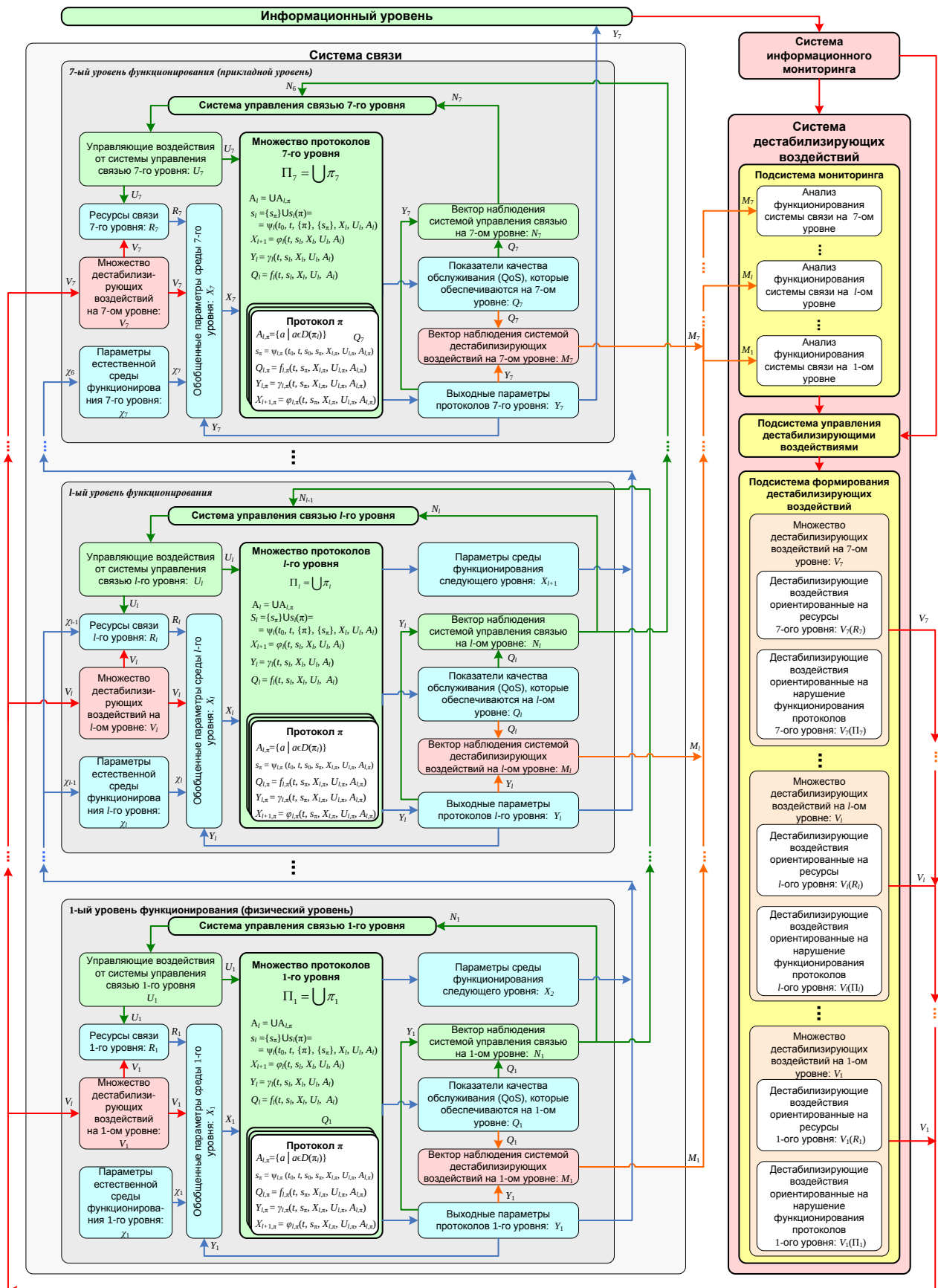


Рис. 4. Многоуровневая иерархическая динамическая модель системы связи в условиях функционально-разноразноуровневого информационного конфликта

Особенности системы связи как пространственно-распределенной системы. В общем случае процессы функционирования системы связи задаются отображениями (26-30) и аналогичны процессу функционирования отдельного протокола, рассмотренному выше. Отличительные особенности иерархического построения системы связи и ее специфика заключаются в следующем. Основу системы связи составляет пространственно-распределенная транспортная сеть, состояние элементов которой и определяет состояние S системы связи в целом:

$$S = \psi(t_0, t, \{S_l\}, X, U, A, Z, E, K, \Lambda, \Theta). \quad (31)$$

Где: $E = \{e_i\}$ – множество средств связи, установленных на узлах сети, при этом каждое средство поддерживает множество протоколов $\{\pi_i\}$, т.е. $e_i = \langle \{\pi_i\} \rangle$;

$Z = \{z_i\}$, – множество узлов сети, каждый узел содержит множество средств связи $\{e_i\}$, т.е. $z_i = \langle \{e_i\}, \{\pi_i\}, \{k_{ij}\} \rangle$;

$K = \{k_{ij}\}$ – множество каналов связи, соединяющих узлы. При этом предполагается, что канал связи $k_{ij} = \langle z_i, z_j, e_i, e_j, \pi_{l,k} \rangle$ соединяет узлы z_i и z_j в случае, если средства связи $e_i \in z_i$ и $e_j \in z_j$, размещенные на этих узлах, используют один и тот же протокол связи $\pi_{l,k}$;

Λ – матрица распределения информационных потоков между абонентами и узлами сети (матрица тяготения).

Параметры $Z \times K$ фактически задают граф сети, а отдельные воздействия $V_{l,\pi}$ за счет нарушения функционирования или блокировки протоколов, используемых как в канале связи $k_{ij} = \langle z_i, z_j, e_i, e_j, \pi_{l,k} \rangle$, так и в узле $z_i = \langle \{e_i\}, \{\pi_i\}, \{k_{ij}\} \rangle$, приводят к изменению данной топологии.

Введем понятия первичной и вторичной структуры сети.

Структура транспортной сети – это формализованное представление сети $\langle Z, K \rangle$, характеризующее связи, реализованные каналаобразующей аппаратурой между узлами системы связи [25].

Информационная структура – это формализованное представление вторичной сети Λ , характеризующее прохождение путей сообщений между узлами, которое реализуется в первичной сети аппаратурой коммутации [25].

Кроме того, целесообразно ввести понятие конфигурации системы связи для формального описания объекта управления.

Конфигурация системы связи — это формализованное представление текущей конфигурации системы связи $S_{conf} = \langle t, Z, K, R, \Pi, A, \Omega, \Lambda \rangle$, описывающее распределение ресурса R на всех ее уровнях L , состава и взаимного расположения каналов и узлов $Z \times K$, оборудования узлов $E \in Z$, протоколов Π , алгоритмов A и их параметров Ω , характеризующее множество транспортных и информационных структур Λ , которые могут быть реализованы в системе связи [25].

Процесс функционирования системы связи определяется отображением $\gamma: \langle t, S, X, U, A \rangle \rightarrow Y$, задаваемым выражением (29). В процессе функционирования системы связи производится доставка сообщений Y_7 с показателями качества Q , что соответствует целевому назначению системы связи в зависимости от ее текущего состояния S и множества входных воздействий X и управления U . Качество выполнения функций по целевому

назначению системы связи определяется показателями Q , которые зависят от множества используемых протоколов Π , функционирующих в соответствии с алгоритмами A и их параметрами Ω , а также зависят от параметров среды $X=R \times \chi \times V$.

Качество функционирования системы связи является ее интегральным свойством, характеризующим способность обеспечивать своевременную, достоверную и безопасную передачу сообщений, в интересах информационно-управляющей системы более высокого уровня.

Качество функционирования определяется как свертка отдельных показателей эффективности системы связи из множества Q на различных уровнях ее функционирования.

В общем случае показатели качества можно классифицировать следующим образом [25]:

- 1) по характеризующим качественным сторонам системы связи:
 - показатели, характеризующие СС как материальный объект:
 - а) готовность;
 - б) устойчивость, определяемая живучестью, помехоустойчивостью и надежностью;
 - в) пропускная способность;
 - г) мобильность;
 - д) безопасность, включающая в себя разведзащищенность и имитостойкость;
 - показатели, характеризующие процессы передачи информации в системе связи:
 - а) своевременность;
 - б) достоверность;
 - в) скрытность;
 - показатели, характеризующие сложность планирования, развертывания и эксплуатации системы связи, отдельных средств связи, средств обеспечения, а также обслуживающего персонала;
 - показатели, характеризующие влияние системы связи на другие смежные системы и метасистему более высокого уровня (определяются задачами системы связи решаемыми ею в структуре информационно-управляющей системы);
- 2) по масштабности характеризующих подсистем:
 - элементарные, характеризующие наименьший элемент системы, к которому они могут быть применены;
 - локальные, характеризующие совокупность элементов или качество отдельного уровня;
 - глобальные, характеризующие отдельные качественные стороны всей системы связи в целом;
- 3) по длительности временного интервала, на котором оценивается система:
 - текущие или точечные, определяемые на элементарном интервале времени;

- интегральные, характеризующие поведение системы на некотором множестве моментов времени (как правило, при $t \rightarrow t_{\text{набл}}$ или $t \rightarrow \infty$);
- 4) по роли в решаемой задаче анализа (синтеза):
 - первичные, задаваемые в виде исходных данных,
 - вторичные - искомые или анализируемые;
 - нейтральные, инвариантные к решаемой задаче;
- 5) по характеризующему элементу динамической модели:
 - состояние системы связи, узлов связи или информационно-управляющей системы в целом;
 - состояние системы управления системы связи;
 - состояние системы воздействия.

Помимо отдельных показателей качества для системы связи как сложной иерархической системы используют интегральные и обобщенные показатели. Интегральные показатели качества вводятся путем свертки отдельных показателей в один. Обобщенные показатели качества характеризуют предпочтительность того или иного состояния в данный момент времени независимо от состояния системы в другой момент времени, а также ее поведение в целом.

Конкретизируем основные показатели качества системы связи на основе работы [25].

- 1) Общие показатели эффективности системы связи:
 - состояния: $q(S)$;
 - точечные: $q(t) = m_t[q(t)]$, где m_t – математическое ожидание показателя q для состояния системы в конкретный момент времени t ;
 - интегральные: $q = m[q(t)]$, где m – математическое ожидание показателя q усредненное по анализируемому интервалу времени. Интегральные показатели представляются через точечные на основе их усреднения по анализируемому интервалу времени.
- 2) Показатели готовности системы связи:
 - состояния - индикаторы готовности
$$q_e(q, T_e) = \begin{cases} 1 & \text{при } \forall \{q(t \geq T_e) \geq q^{\text{треб}}\} \\ 0 & \text{при } \exists \{q(t \geq T_e) < q^{\text{треб}}\} \end{cases};$$
 - точечные — вероятность готовности в момент времени t
$$q(t) = m_t[q(t)] = P(q(S, t) \geq q^{\text{треб}});$$
 - интегральные — вероятность готовности в случайно выбранный момент t
$$q = m[q(t)] = P(q(S) \geq q^{\text{треб}}).$$
- 3) Показатели пропускной способности системы связи:
 - состояния:
 - а) связность направления связи;
 - б) пропускная способность направления связи;
 - в) коэффициент реализации требований информационно-управляющей системы более высокого уровня по пропускной способности и связности направления связи;

- точечные:
 - а) математическое ожидание пропускной способности и связности направления в момент времени t ;
 - б) математическое ожидание коэффициента реализации требований по пропускной способности и связности направления в момент времени t ;
- интегральные:
 - а) математическое ожидание пропускной способности и связности направления за наблюдаемый период времени $t_{\text{набл}}$;
 - б) математическое ожидание коэффициента реализации требований по пропускной способности и связности направления за наблюдаемый период $t_{\text{набл}}$.

4) Показатели устойчивости системы определяются на основе введения функций, характеризующих случайные изменения среды (χ) или преднамеренные воздействия (V), обуславливающие ухудшение показателей качества системы связи: $q_1(X) \rightarrow q_2(X, V)$, $q_1 \geq q_2$.

- показатели устойчивости состояния:
 - а) коэффициент, определяющий уменьшение показателей качества состояния системы при наихудшем воздействии V

$$k_u(q, V) = \inf \left(\frac{q}{q(V)} \right);$$

- б) величина, определяющая уровень воздействия V , необходимого для изменения показателей качества системы ниже требуемого значения

$$\Delta V = \inf V \mid \exists \{q(X, V) < q^{\text{треб}}\};$$

- в) индикатор устойчивости состояния – определяет вероятность соответствия всех показателей качества системы связи $Q = \{q\}$ требуемым значениям

$$k_u = P(\forall \{q \geq q^{\text{треб}}\}). \quad (30)$$

В более простом случае в качестве индикатора устойчивости можно использовать признак снижения любого из показателей качества ниже требуемого значения

$$k_u = \begin{cases} 1 & \text{при } \forall \{q \geq q^{\text{треб}}\} \\ 0 & \text{при } \exists \{q < q^{\text{треб}}\} \end{cases}.$$

С учетом того, что для различных уровней функционирования системы связи свойственна свертка показателей качества

$$Q_1 \rightarrow Q_2 \rightarrow \dots \rightarrow Q_i \rightarrow \dots \rightarrow Q_7,$$

то при рассмотрении устойчивости системы связи конкретного l -ого уровня можно ограничиться сверткой до этого уровня

$$k_{ul} = P(\forall \{Q_l \geq Q_l^{\text{треб}}\}). \quad (31)$$

- Точечные показатели устойчивости:
 - 1) определяются и интерпретируются аналогично рассмотренным выше в соответствии с выражением (30), (31);

- 2) среднее ожидаемое в момент t значение коэффициента потери качества за время Δt (математическое ожидание вычисляется по совместному распределению показателей $q(t)$, $q(t+\Delta t)$ системы в моменты времени t и $t+\Delta t$)

$$\Delta k_u(\Delta t) = [q(t) - q(t+\Delta t)]/q(t);$$

- 3) время Δt , через которое ожидаемое значение показателей качества снизится ниже требуемого значения

$$\Delta t \mid q(t+\Delta t) < q^{треб}.$$

Интегральные показатели устойчивости. К основным показателям устойчивости, представляющим интерес, можно отнести зависимости конкретных показателей качества q от преднамеренных воздействий V при управлении U . Такая оценка позволяет вывести следующие показатели:

- устойчивость системы связи к воздействиям V ;
- устойчивость системы связи к случайным возмущениям среды функционирования χ ;
- устойчивость системы связи к подавлению некоторого протокола связи π ;

Показатели полноты наблюдаемости, скрытности и разведзащищенности (как свойства определяющие возможности по наблюдению со стороны противника) анализируются при формализации конфликта системы связи и системы воздействия. Показатели мобильности, своевременности и достоверности являются внутренними показателями системы связи и учитываются в векторе Q .

В составе показателей качества, применяемых в математических моделях для описания структуры и процесса функционирования системы связи, наряду с вышеуказанными показателями могут выделяться и описываться показатели, соответствующие взаимодействию системы, среды функционирования и других объектов (систем наблюдения и воздействия противника). При этом задача анализа системы связи на ее динамической модели сводится к нахождению временной зависимости показателей эффективности, заданных на состоянии исследуемого объекта, и определению по ним точечных и интегральных показателей системы [25].

Система связи является эффективно функционирующей в случае если ее показатели качества верхнего (прикладного) уровня Q_7 , получаемые в результате свертки

$$Q_1 \rightarrow Q_2 \rightarrow \dots \rightarrow Q_i \rightarrow \dots \rightarrow Q_7,$$

имеют значения не ниже требуемого, то есть выполняется критерий

$$\forall \{q_7 \geq q_7^{треб}\} \in Q_7. \quad (32)$$

При этом особое значение имеют четыре нижних уровня: физический, каналный, сетевой и транспортный, которые соответствуют телекоммуникационному оборудованию системы связи и в большей степени уязвимы для преднамеренных воздействий. Поэтому в качестве частного случая можно рассматривать систему связи как пространственно-распределенную

транспортную сеть ограниченную четырьмя нижними уровнями OSI. В этом случае критерий (32) может быть представлен в виде

$$\forall \{q_4 \geq q_4^{\text{треб}}\} \in Q_4. \quad (33)$$

Особенности построения каналов наблюдения системы связи со стороны системы управления и системы воздействий. Применительно к системе связи в целом канал наблюдения N со стороны системы управления связью должен включать в себя не только наблюдаемые параметры Q и Y ($N=UN_l=<Q_N \times Y_N>$), но и конфигурацию системы связи $S_{\text{conf}}=<t, Z, K, R, \Pi, A, \Omega, \Lambda>$, включающую в себя протоколы Π , алгоритмы A и их параметры Ω , топологию системы связи $Z \times K$, структуру передачи информационных потоков Λ и распределение ресурсов R . Фактически полную формализацию канала наблюдения можно представить в виде

$$N \times S_{\text{conf}},$$

где: N – наблюдаемые показатели качества, S_{conf} – управляемые параметры системы связи, причем управляемые как со стороны системы управления связью, так и со стороны системы дестабилизирующих воздействий.

По аналогии с каналом N , канал наблюдения системы связи со стороны противника M также должен включать в себя помимо показателей Q и Y ($M=UM_l=<Q_M \times Y_M>$) показатели, характеризующие вскрытие и идентификацию протоколов функционирования системы связи $\Pi=U\Pi_l$, ее транспортной структуры $<Z, K>$, а также информационной структуры Λ , определяемой маршрутами передачи информационных потоков. Идеальным вариантом для противника является полное наблюдение конфигурации системы связи $S_{\text{conf}}=<t, Z, K, R, \Pi, A, \Omega, \Lambda>$. Однако фактически наблюдаемая конфигурация $S_{\text{набл}}^{\text{набл}}$ будет неполной $S_{\text{набл}}^{\text{набл}} \subset S_{\text{conf}}$.

В таком случае канал наблюдения со стороны системы воздействий формально можно представить в виде

$$M \times S_{\text{набл}}^{\text{набл}}.$$

В процессе функционирования канала наблюдения $M \times S_{\text{набл}}^{\text{набл}}$ со стороны системы воздействия формируется так называемая «картина наблюдения» (процесс $M \times S_{\text{набл}}^{\text{набл}} \times t_{\text{набл}}$), идентифицирующая с определенной вероятностью (достоверностью) элементы S_{conf} . Идентификация, как правило, ведется по признаковому пространству каждого объекта. В соответствии с наблюдаемыми признаками каждый элемент конфигурации $S_{\text{набл}}^{\text{набл}}$ относится к некоторому, заранее заданному классу с определенной степенью достоверности. Процесс такого сопоставления, а также задачи выбора множества признаков и методики классификации объектов $S_{\text{набл}}^{\text{набл}}$ за время $t_{\text{набл}}$ относятся к самостоятельным научным задачам, решаемым на основе теорий кластеризации и классификации.

Система управления связью и система дестабилизирующих воздействий. Функционирование системы связи, как правило, сопровождается динамическим или стохастическим изменением значений множества входных параметров на различных ее уровнях $X=UX_l$, $X_l=<R_l \times \chi_l \times V_l>$, которые в условиях

информационного конфликта в первую очередь определяются множеством преднамеренных воздействий на различных уровнях $V=UV_l$.

Для обеспечения выполнения критерия (32) по соответствию качества связи заданным значениям на протоколы Π со стороны системы управления связью оказывается множество управляющих воздействий $U=UU_l$, которые, как правило, связаны или с распределением ресурсов R_l на различных уровнях, или с изменением параметров Ω алгоритмов A , на основе которых функционируют протоколы системы связи.

Управление системой связи характеризуется рядом особенностей. Для динамической модели системы связи наиболее существенными из них являются [25]:

- наличие совокупности направлений связи, в которых обеспечивается обмен сообщениями абонентов и узлов;
- возможность использования различных путей прохождения сообщений в рамках одного направления связи;
- зависимость множества реализуемых информационных путей передачи информации Λ от транспортной структуры $\langle Z, K \rangle$ и конфигурации системы связи S_{conf} ;
- инерционность процессов управления состояниями транспортной и информационной структур, а также процессов изменения конфигурации системы связи.

Множество управляющих воздействий U направляется на перестройку (создание) топологии системы связи $Z \times K$, преобразование структур транспортной S и информационной Λ сетей, управление резервами R , протоколами средств связи Π (режимами помехозащиты, рабочими частотами, мощностью передачи, видом формируемых сигналов и способом их обработки) и т.д. Особенностью построения системы управления связью является то, что она с одной стороны функционально разобщена по уровням функционирования (что приводит к тому, система управления каждого уровня стремиться обеспечить выполнение только своих задач), а с другой стороны должна обеспечивать требуемое качество связи $Q^{треб}$ в интересах информационно-управляющей системы более высокого уровня. Иерархический характер управления означает, что в рамках одного состояния системы связи, определяемого старшим элементом подсистемы управления (высшего уровня иерархии), допускается управление младшими элементами и состояниями системы связи на более низких уровнях иерархии. Процессы управления различных уровней иерархии различаются по масштабности и сложности решаемых задач, по степени их влияния на систему связи и информационно-управляющую систему в целом, по динамичности, уровню автоматизации и другим показателям. Все вышеуказанное, а также принцип функциональной независимости уровней, введенный моделью OSI, позволяют рассматривать управление ресурсами отдельного уровня независимо от других.

Традиционно процессы функционирования системы связи, управления ее ресурсами и конфликт с системой дестабилизирующих воздействий рассматриваются на каком-либо одном уровне модели OSI. Анализ работ в

области РЭП [1, 3-37] и информационного противоборства в технической сфере [38-78] показал, что преднамеренным воздействиям в основном подвергаются четыре нижних уровня транспортной подсистемы модели OSI.

Как правило, авторы для системы связи рассматривают либо одноуровневый информационный конфликт (рис. 4а, б), либо многоуровневые эффекты на различных уровнях системы связи в условиях одноуровневого воздействия (рис. 4в). Вместе с тем для перспективных систем дестабилизирующих воздействий нельзя исключать применения разноуровневого комплексного воздействия (рис. 4г).

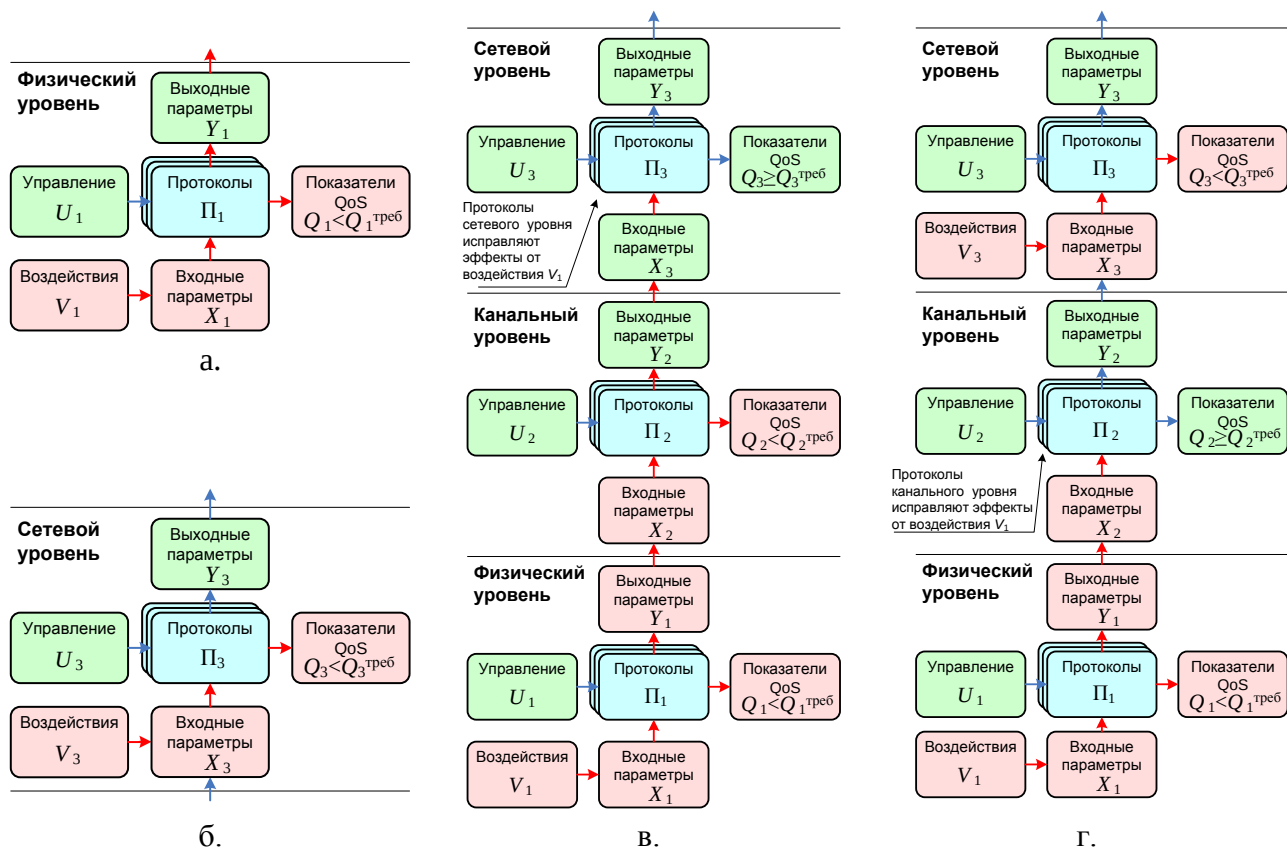


Рис. 4. Информационный конфликт по уровням воздействия:

- а) воздействие только на физическом уровне (например, РЭП);
- б) воздействие только на сетевом уровне (например, DDOS-атаки);
- в) оценка эффектов от одноуровневого воздействия на физическом уровне (например, эффекты от РЭП приводят к потери достоверности приема, которую не способны исправить протоколы физического и канального уровня, но за счет перемаршрутизации на сетевом уровне эффекты от воздействия исправляются);
- г) разноуровневое комплексное воздействие (по аналогии с предыдущим случаем, только дополнительное использование ИТВ на сетевом уровне приводит к нестабильному функционированию протоколов маршрутизации и доставка пакетов невозможна).

При этом наиболее вероятным сценарием является использование на нижних уровня не критичных динамических воздействий ($Q_1(V_1) > Q_1^{\text{треб}}$), эффект которых отображается на более верхние уровни ($V_1 \rightarrow X_1 \rightarrow \Pi_1 \rightarrow Y_1 \rightarrow X_2 \rightarrow \Pi_2 \rightarrow \dots$) и «раскачивает» систему связи, переводя ее в погранично-устойчивое

состояние. Одновременно на верхних уровнях (например, сетевом или транспортном) используются точечные информационно-технические воздействия V_i , ориентированные на блокировку или нарушение функционирования критических протоколов связи, что приводит к потере устойчивости всей системы $Q(V_1, V_i) < Q^{\text{треб}}$ (рис. 5б).

Наличие одновременных разноуровневых воздействий, а также глубокая функциональная взаимосвязь между уровнями системы связи требует реализации единой стратегии управления $U = U U_i$ на различных уровнях иерархии. Реализация такого управления требует создания метасистемы управления, которая бы обеспечивала управление каждым из уровней с квази-оптимальной стратегией суммарных затрат ресурсов всех уровней $R(U, V) \rightarrow \min$. Причем данное управление должно быть адаптивным к преднамеренным воздействиям V .

Например, применение корректирующего кодирования позволяет избежать многократного повышения полосы частот канала при одинаковой достоверности приема. А изменение маршрутов передачи в сети позволит избежать передачи данных по каналам, на которые оказываются преднамеренные воздействия, вместо того чтобы тратить частотно-временные и энергетические ресурсы физического и канального уровня на обеспечение их требуемой помехозащищенности.

Управление U в общем случае должно соответствовать принципу компенсации из теории управления по отношению к преднамеренным воздействиям V и условиям среды χ . При этом компенсация может быть:

- *активной* за счет непосредственной выдачи управляющих воздействий U_i на соответствующие объекты управления (см. выше);
- *пассивной* за счет внесения некоторой избыточности (количественной, функциональной или временной) в математическое обеспечение A , в их параметры Ω протоколов Π , в структуру взаимодействия протоколов, а также в ресурсы системы связи R . Это позволит обеспечить выполнение требований $Q \geq Q^{\text{треб}}$ в более широком диапазоне входных параметров $X = \langle R \times \chi \times V \rangle$ и сократить интенсивность выдачи управляющих воздействий U .

Особенности управления и воздействия на систему связи как на многоуровневую иерархическую систему. Как показано в работе [99] эффективность управления многоуровневой системы, каковой является система связи, зависит от соотношений между глобальной и локальными целями функционирования на каждом из уровней. В самом деле, стремление локальных систем управления каждого уровня минимизировать свои собственные целевые функции $R_i(U_i) \rightarrow \min \mid Q_i \geq Q_i^{\text{треб}}$ может не приводить к достижению глобального оптимума $R(U) \rightarrow \min$. В связи с этим может возникнуть межуровневая несогласованность (конфликт) между локально принимаемыми решениями. Принципы координации иерархических систем, представленные в работе [99], показывают, что при принятии локальных решений необходимо выполнение условий координируемости.

В общем случае в многоуровневой системе возникают два вида конфликтов [99]:

- межуровневые;
- внутриуровневые.

Межуровневый конфликт есть конфликт между двумя различными уровнями в многоуровневой системе и характеризуется невозможностью достижения глобальной цели за счет реализации локальных задач уровней. Например, если глобальной целью является максимизация пропускной способности системы, а локальными целями является минимизация затрат ресурса на всех уровнях, то возникает конфликт между уровнями [99].

Внутриуровневый конфликт представляет собой конфликт в пределах отдельного уровня. Данный конфликт возникает когда достижению локальной цели уровня препятствует некоторый элемент [99]. Особенности таких конфликтов рассмотрены в работах Угольницкого Г.А. [111], Усова А.Б. [112] и Деттмера У. [113].

В связи с указанными особенностями управления в системе связи к перспективным способам преднамеренного воздействия можно отнести многоуровневые или одноуровневые воздействия, ориентированные на:

- порождение или развитие межуровневых конфликтов в системе связи;
- порождение или развитие внутриуровневых конфликтов в системе связи.

Воздействия, ориентированные на внутриуровневые конфликты в системе связи, могут быть реализованы за счет нарушения логики работы или функциональной блокировки отдельных «ключевых» протоколов или элементов системы связи на данном уровне. Воздействия, ориентированные на межуровневые конфликты, могут быть реализованы за счет учета отображений эффекта от воздействия на вышестоящие уровни системы или с использованием многоуровневых воздействий, ориентированных на «ключевые» протоколы системы связи.

Гипотеза о нарушении эффективности функционирования системы связи за счет применения совокупности разноуровневых неэффективных воздействий

Как показано выше система связи является эффективной в случае, если ее показатели качества верхнего (прикладного) уровня Q_7 , получаемые в результате свертки

$$Q_1 \rightarrow Q_2 \rightarrow \dots \rightarrow Q_i \rightarrow \dots \rightarrow Q_7,$$

имеют значения не ниже требуемого, то есть выполняется критерий:
 $\forall \{q_7 \geq q_7^{\text{треб}}\} \in Q_7$.

По аналогии введем понятие *эффективных условий функционирования* – условий $X_{эф} = U X_l$ ($X_l = \langle R_l \times \chi_l \times V_l \rangle$), которые при управлении системой связи $U = U U_l$ обеспечивают выполнение критерия эффективности функционирования $\forall \{q_7 \geq q_7^{\text{треб}}\}$. Существование таких эффективных условий определяет область *неэффективных воздействий* – то есть воздействий $V_{неф} = U V_l$, которые при управлении $U = U U_l$ не способны вывести систему за пределы эффективного

функционирования, то есть $Q(U, X_{эф}(V_{нэф})) \geq Q^{тр\epsilonб}$. Другими словами эффективные условия функционирования системы связи соответствуют условию неэффективных воздействий.

В настоящее время в модели OSI принят *классический принцип независимости протоколов системы связи на различных уровнях ее функционирования*. В основу классического принципа многоуровневого функционирования в соответствии с моделью OSI положены два положения:

- 1) Протоколы вышестоящих уровней Π_l и система управления ими U_l должны обеспечивать исправление неэффективных выходных параметров (выходных условий) нижестоящих уровней $Y_{l-1 \text{ нэф}} \rightarrow X_{l \text{ эф}}$

$$\varphi_l : Y_{l-1 \text{ нэф}} \xrightarrow{\Pi_l} \begin{bmatrix} X_{l \text{ эф}} \\ X_{l \text{ нэф}} \end{bmatrix}, \quad (34)$$

$X_{l \text{ эф}}$ – соответствует, случаю когда протоколы Π_l исправляют неэффективные условия функционирования предыдущего уровня; $X_{l \text{ нэф}}$ – когда не исправляют. При этом

$$X_{l \text{ нэф}} = \bigcup_{\Pi_l} X_{l, \pi \text{ нэф}}, \quad X_{l \text{ эф}} = \bigcup_{\Pi_l} X_{l, \pi \text{ эф}}, \quad \text{и в итоге } X_l = X_{l \text{ эф}} \cup X_{l \text{ нэф}}.$$

- 2) На своем уровне функционирования протоколы Π_l функционально независимы от нижестоящих уровней Π_{l-1} и должны обеспечивать требуемую эффективность функционирования:

$$f_l : \langle t, s_l, X_{l \text{ эф}}, U_l, A_l \rangle \xrightarrow{\Pi_l} Q_l \mid Q_l \geq Q_l^{тр\epsilonб}. \quad (35)$$

Выражение (34) позволяет сформировать следствие, на первый взгляд кажущееся логичным – если выходные параметры протоколов нижестоящего уровня $Y_{l-1 \text{ нэф}}$ являются эффективными $Y_{l-1} = Y_{l-1 \text{ эф}}$, то и условия функционирования протокола вышестоящего уровня являются эффективными:

$$Y_{l-1 \text{ эф}} \Rightarrow X_{l \text{ эф}}, \quad (36)$$

откуда, распространяя данный вывод на все уровни системы связи получаем, что эффективные условия 1-го уровня служат причиной эффективных условий всех последующих уровней.

$$X_{1 \text{ эф}} \Rightarrow Y_{1 \text{ эф}} \Rightarrow \dots \Rightarrow Y_{l-1 \text{ эф}} \Rightarrow X_{l \text{ эф}} \Rightarrow \dots \Rightarrow Y_{7 \text{ эф}}. \quad (37)$$

Вместе с тем, из практики связи известно, что существуют режимы функционирования протоколов связи, которые являются неэффективными, но при этом соблюдаются условия эффективного функционирования 1-го уровня: $X_{1 \text{ эф}} \Rightarrow X_{i \text{ нэф}}$. Таким образом, следствие (37) – не выполняется. Как правило, объяснение наличия таких условий лежит в области независимости функциональных уровней системы связи и, якобы, невозможности формирования отдельных условий текущего уровня из условий функционирования предыдущего уровня. Однако, по мнению автора, это не совсем верно.

Введем *принцип расширенной оценки условий функционирования протоколов системы связи на различных ее уровнях*, который направлен на разрешение сформулированного противоречия.

Для устранения противоречия необходимо изменить строгость допущений (34), и ввести условия, когда эффективные выходные параметры протоколов нижестоящих уровней $Y_{l-1 \text{эф}}$ могут определять неэффективные условия функционирования протоколов вышестоящего уровня $X_{l \text{нэф}}$:

$$\left\{ \begin{array}{l} \varphi_l : Y_{l-1 \text{нэф}} \xrightarrow{\Pi_l} \begin{bmatrix} X_{l \text{эф}} \\ X_{l \text{нэф}} \end{bmatrix} \\ \varphi_l : Y_{l-1 \text{эф}} \xrightarrow{\Pi_l} \begin{bmatrix} X_{l \text{эф}} \\ X_{l \text{нэф}} \end{bmatrix} \end{array} \right. . \quad (38)$$

Отсюда следует оригинальный вывод о существовании эффективных выходных параметров $Y_{l-1 \text{эф}}$ и условий функционирования $X_{l-1 \text{эф}}$ нижестоящих уровней, которые являются причиной неэффективных условий $X_{l \text{нэф}}$ на вышестоящих уровнях системы связи:

$$\begin{aligned} \exists Y_{l-1 \text{эф}} &\Rightarrow X_{l \text{нэф}} , \\ \exists X_{l \text{эф}} &\Rightarrow Y_{l-1 \text{эф}} \Rightarrow X_{l \text{нэф}} . \end{aligned} \quad (39)$$

Распространяя данный вывод на все L уровни системы связи получаем, что существуют такие эффективные условия функционирования любого из уровней $X_{i \text{эф}}$, которые могут служить причиной неэффективных условий функционирования $X_{j \text{эф}}$ ($j > i$) любого из последующих уровней. В случае, если эти неэффективные условия не исправляются вышестоящим уровнем функционирования, система связи оказывается функционально подавленной:

$$\exists X_{1 \text{эф}} \Rightarrow Y_{1 \text{эф}} \Rightarrow X_{2 \text{эф}} \Rightarrow \dots \Rightarrow X_{l \text{нэф}} \Rightarrow Y_{l \text{нэф}} \Rightarrow \dots \Rightarrow X_{7 \text{нэф}} . \quad (40)$$

В общем случае причиной создания таких неэффективных условий могут быть как внутрисистемные конфликты в системе связи, так и преднамеренные воздействия на систему связи.

Для преднамеренной реализации вышеприведенных условий неэффективного функционирования системы связи можно предложить три базовых варианта воздействия.

- 1) Воздействие на нижестоящем уровне V_i , которое неэффективно на i -ом уровне (то есть не ведет к снижению $Q_i < Q_i^{\text{треб}}$), но за счет отображения $V_{i \text{нэф}} \rightarrow X_{i \text{эф}} \rightarrow Y_{i \text{эф}} \rightarrow \dots \rightarrow X_{j \text{нэф}} \rightarrow Y_{j \text{нэф}}$ на вышестоящий j -ый уровень системы связи формирует его неэффективную среду $X_{j \text{нэф}}$, приводящую к критическому падению качества функционирования этого уровня ($Q_j < Q_j^{\text{треб}}$) или всей системы ($Q < Q^{\text{треб}}$). См. рис. 5а.
- 2) Совокупность воздействий $V = UV_i$ на различных уровнях которые по отдельности неэффективны, но за счет их отображения на вышестоящие уровни создает эффект неэффективных условий среды $X_{j \text{нэф}}$ на вышестоящем j -ом уровне (рис. 5б):

$$\begin{array}{ccccccc} & & & V_{i-1 \text{нэф}} & & V_{i \text{нэф}} & \\ & & & \downarrow & & \downarrow & \\ X_{1 \text{эф}} & \rightarrow & Y_{1 \text{эф}} & \rightarrow & \dots & \rightarrow & X_{i-1 \text{эф}} \rightarrow Y_{i-1 \text{эф}} \rightarrow X_{i \text{эф}} \rightarrow Y_{i \text{эф}} \dots \rightarrow X_{j \text{нэф}} \rightarrow Y_{j \text{нэф}} \end{array} .$$

3) Одиночные воздействия V_i или их совокупность $V=UV_i$ на различных уровнях, приводящие к возникновению и развитию внутрисистемных конфликтов в системе связи как внутри отдельного уровня (рис. 5в), так и между уровнями функционирования (рис. 5г).

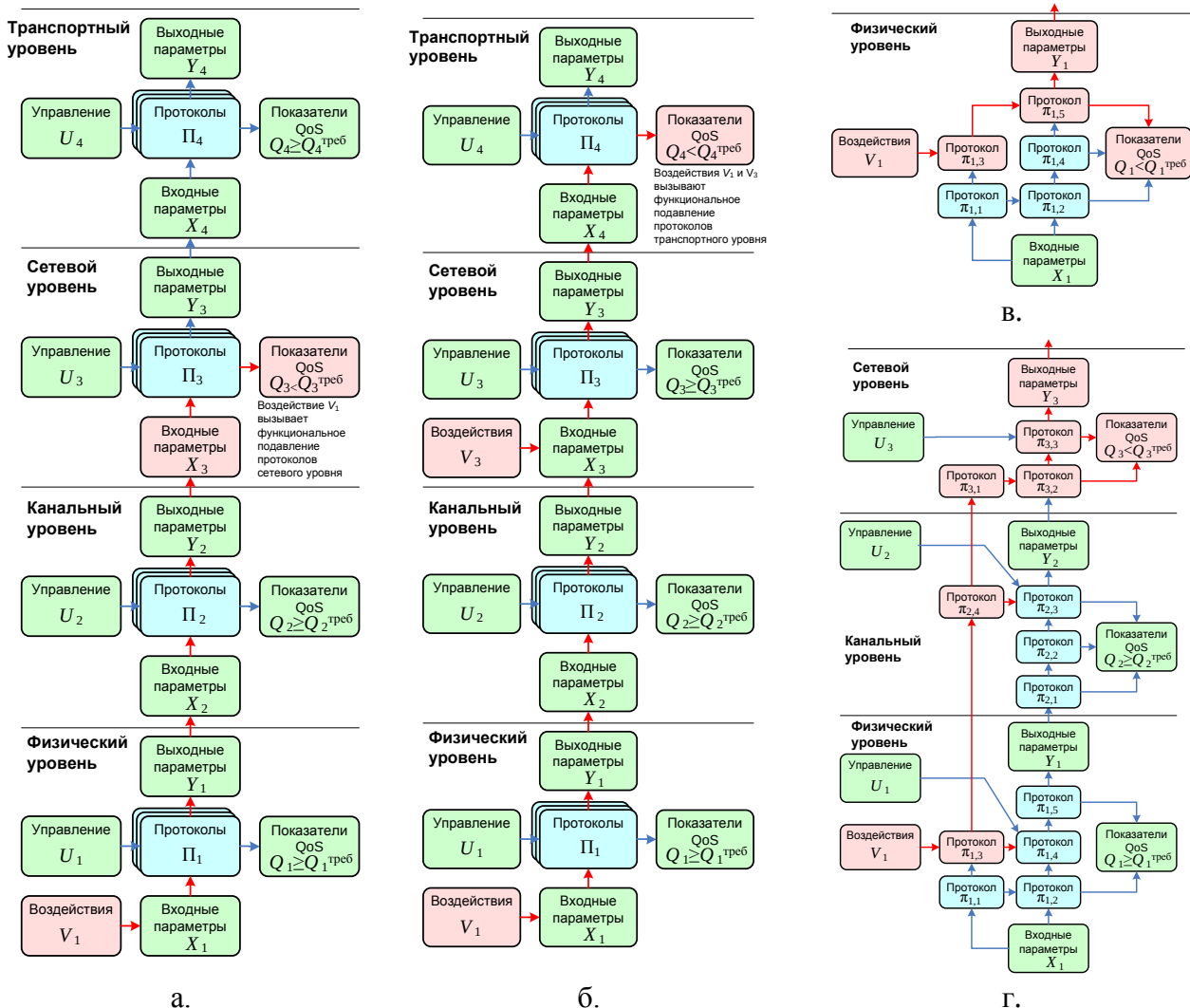


Рис. 5. Новые варианты дестабилизирующих воздействий на систему связи:

- а) воздействие, на нижестоящем уровне, которое за счет отображения на вышестоящий уровень системы связи формирует его неэффективную среду функционирования;
- б) совокупность воздействий на различных уровнях которые по отдельности неэффективны, но за счет их отображения на вышестоящие уровни создает эффект неэффективных условий среды;
- в) воздействие приводящие к возникновению и развитию внутрисистемных конфликтов в системе связи на одном уровне;
- г) воздействие приводящие к возникновению и развитию внутрисистемных конфликтов в системе связи на различных ее уровнях.

В случае разработки подобных базовых вариантов воздействий их реализация будет носить скрытно-бескомпроматный характер, так как идентификация факта такого воздействия потребует от системы управления связью наблюдения не только за параметрами Q_i и Y_i на отдельных уровнях, но

и наблюдения за поведением отображений ψ_l, γ_l, f_l внутри каждого из уровней, а также за поведением отображений φ_l между уровнями.

Вывод

В работе представлена динамическая модель информационного конфликта системы связи и системы дестабилизирующих воздействий, которая обобщает ранее опубликованные работы для случаев воздействия средств РЭП и ИТВ. Рассмотрены случаи обобщения одновременного воздействия РЭП и ИТВ как многоуровневых воздействий, проведена формализация таких конфликтов. На основе предложенной модели теоретически обоснован новый вид информационных конфликтов на основе функционально-разноуровневых воздействий, приводящих к функциональному подавлению системы связи за счет создания в ней внутрисистемных конфликтов.

Исследование информационного конфликта выполнены при государственной поддержке РФФИ инициативного научного проекта № 13-07-97518 и поддержке Департаментом приоритетных направлений науки и технологий Минобрнауки РФ – грантом Президента РФ № МК-755.2012.10.

Автор выражает благодарность д.т.н. доценту Новикову Е.А. за плодотворное обсуждение материалов и Ушаневу К.В. за помощь в подготовке текста статьи.

Литература

1. Будников С. А., Гревцев А. И., Иванцов А. В., Кильдюшевский В. М., Козирацкий А. Ю., Козирацкий Ю. Л., Кущев С. С., Лысиков В. Ф., Паринов М. Л., Прохоров Д. В. Модели информационного конфликта средств поиска и обнаружения. Монография / Под ред. Ю.Л. Козирацкого. – М.: Радиотехника, 2013. – 232 с.
2. Новиков Д. А. Иерархические модели военных действий // Управление большими системами. 2012. № 37. С. 25-62.
3. Владимиров В. И., Владимиров И.В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). – Воронеж: ВАИУ, 2008. – 231 с.
4. Козирацкий Ю. Л., Подлужный В. И., Паринов М. Л. Методический подход к построению вероятностной модели конфликта сложных систем // Вестник ВИРЭ. 2005. № 3. С. 4-16.
5. Зюко А.Г. Помехоустойчивость и эффективность систем связи. – М.: Связь, 1972. – 359 с.
6. Максимов М. В., Бобнев М. П., Кривицкий Б. Х., Горгонов Г.И., Степанов Б. М., Шустов Л. Н., Ильин В. А. Защита от радиопомех / Под ред. М.В. Максимова. – М.: Сов. радио, 1976. – 496 с.
7. Коржик В. И., Финк М. М., Щелкунов К. Н. Расчет помехоустойчивости систем передачи дискретной информации. Справочник. – М.: Радио и связь, 1981. – 267 с.

8. Тузов Г. И., Сивов В. А., Прытков В. И. и др. Помехозащищенность радиосистем со сложными сигналами / Под ред. Г.И. Тузова. – М.: Радио и связь, 1985. – 264 с.
9. Палий А. И. Радиоэлектронная борьба. – М.: Воениздат, 1989. – 350 с.
10. Перунов Ю. М., Мацукевич В. В., Васильев А. А. Зарубежные радиоэлектронные средства. В 4-х книгах. Книга 2: Системы радиоэлектронной борьбы. – М.: Радиотехника, 2010. – 352 с.
11. Современная радиоэлектронная борьба. Вопросы методологии / Под ред. В.Г. Радзиевского. – М.: Радиотехника, 2006. – 424 с.
12. Куприянов А. И., Сахаров А. В. Радиоэлектронные системы в информационном конфликте. – М.: Вузовская книга, 2003. – 528 с.
13. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. – М.: Вузовская книга, 2011. – 800 с.
14. Куприянов А. И. Радиоэлектронная борьба. – М.: Вузовская книга, 2013. – 360 с.
15. Борисов В. И., Зинчук В. М. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. – М.: Радио и связь, 1999. – 252 с.
16. Борисов В. И., Зинчук В. М., Лимарев А. Е., Немчилов А. В., Чаплыгин А. А. Пространственные и вероятностно-временные характеристики эффективности станций ответных помех при подавлении систем радиосвязи / Под ред. В.И. Борисова. – Воронеж: ОАО «Концерн «Созвездие», 2007. – 354 с.
17. Владимиров В. И. Принципы и аппарат системных исследований радиоэлектронного конфликта. Учебное пособие. – Воронеж: ВВВИУРЭ, 1992.
18. Владимиров В. И., Гальянов Г. П. Эффективность комплексов РЭП и методы ее оценки. Учебное пособие. – Воронеж: ВВВИУРЭ, 1993.
19. Владимиров В. И., Гостев В. А. Основы радиоподавления, построения и применения средств и комплексов РЭП систем передачи информации. Часть 2. Курс лекций. – Воронеж: ВИРЭ, 1997.
20. Владимиров В. И. Информационные основы радиоподавления линий радиосвязи в динамике радиоэлектронного конфликта. – Воронеж: ВИРЭ, 2003. – 276 с.
21. Владимиров В. И., Лихачев В. П., Шляхин В.М. Антагонистический конфликт радиоэлектронных систем. – М.: Радиотехника, 2004. – 384 с.
22. Семисошенко М. А. Управление автоматизированными сетями декаметровый связи в условиях сложной радиоэлектронной обстановки. – СПб.: ВАС, 1997. – 364 с.
23. Чуднов А. М. Анализ помехозащищенности линий и сетей связи. – Л.: ВАС, 1988. – 34 с.
24. Чуднов А. М. Помехоустойчивость линий и сетей связи в условиях оптимизированных помех. – Л.: ВАС, 1986. – 84 с.
25. Барашков П. Н., Родимов А. П., Ткаченко К. А., Чуднов А. М. Модель системы связи с управляемыми структурами в конфликтных условиях. – Л.: ВАС, 1986. – 52 с.

26. Бураченко Д. Л. Оптимальное разделение цифровых сигналов многих пользователей в линиях и сетях связи в условиях помех. – Л.: ВАС, 1990. – 302 с.
27. Кузнецов В. И. Радиосвязь в условиях радиоэлектронной борьбы. – Воронеж.: ВНИИС, 2002. – 403 с.
28. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.
29. Исаков Е. Е. Устойчивость военной связи в условиях информационного противоборства. – СПб.: Изд-во Политехн. ун-та, 2009. – 400 с.
30. Одоевский С. М., Калюка В. И. Адаптивно-игровое моделирование военных сетей беспроводного абонентского доступа. В 2-х частях. Часть 1. – Новочеркасск: УПЦ «Набла» ЮРГТУ (НПИ), 2009. – 216 с.
31. Николаев В. И., Фёдоров А. Е. Функционирование цифровых систем связи в условиях радиоэлектронного конфликта с минимаксных позиций теории игр (часть 1) // Теория и техника радиосвязи. 2010. № 2. С. 37-43.
32. Николаев В. И., Фёдоров А. Е. Функционирование цифровых систем связи в условиях радиоэлектронного конфликта с минимаксных позиций теории игр (часть 2) // Теория и техника радиосвязи. 2010. № 2. С. 44-49.
33. Шабалин Е. А. Способы повышения эффективности систем радиосвязи в условиях конфликта // Электросвязь. 2008. № 9. С. 40-44.
34. Шабалин Е. А., Милов В. Р. Распределение ресурсов сети связи с учетом ценности информации в условиях радиоэлектронного противодействия // Информационно-измерительные и управляющие системы. 2008. № 11. С. 87-93.
35. Радько Н. М., Мокроусов А. Н. Динамическая модель работы адаптированного к помехам радиосредства с использованием сетей Петри // Информация и безопасность. 2009. № 2. С. 257-262.
36. Мальцев Г. Н., Вознюк В. В., Туктамышев М. Р. Моделирование конфликта сложных радио-технических систем методом параллельных развивающихся стохастических процессов // Информационно-управляющие системы. 2013. № 5. С. 26-33.
37. Радзиевский В. Г., Сирота А. А. Информационное обеспечение радиоэлектронных систем в условиях конфликта. – М.: ИПРЖР, 2001. – 456 с.
38. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Военная мысль. 2012. № 7. С. 22-31.
39. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Информационные системы и технологии. 2011. № 1. С. 80-85.
40. Стародубцев Ю. И., Семенов С. С., Бухарин В. В. Техносферная война // Научно-информационный журнал Армия и общество. 2010. № 4. С. 6-11.
41. Семенов С. С., Гусев А. П., Барботько Н. В. Оценка информационно-боевого потенциала сторон в техносферных конфликтах // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 6. С. 10-21.
42. Новиков Д. А., Чхартишвили А. Г. Рефлексивные игры. – М.: СИНТЕГ, 2003. – 149 с.

43. Новиков Д. А., Чхартишвили А. Г. Прикладные модели информационного управления. – М.: ИПУ РАН, 2004. – 129 с.
44. Новиков Д. А. Сетевые структуры и организационные системы. – М.: ИПУ РАН, 2003. – 102 с.
45. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. Д.А. Новикова. – М.: Издательство физико-математической литературы, 2010. – 228 с.
46. Расторгуев С. П. Математические модели в информационном противоборстве. Экзистенциальная математика. – М.: АНО ЦСОиП, 2014. – 260 с.
47. Бирюков Д. Н., Ростовцев Ю. Г. Подход к построению непротиворечивой теории синтеза сценариев упреждающего поведения в конфликте // Труды СПИИРАН. 2015. № 1. С. 94-111.
48. Бирюков Д. Н., Ломако А. Г. Подход к построению ИБ-систем, способных синтезировать сценарии упреждающего поведения в информационном конфликте // Защита информации. Инсайд. 2014. № 6 (60). С. 42-49.
49. Бирюков Д. Н., Ломако А. Г., Сабиров Т. Р. Многоуровневое моделирование сценариев упреждающего поведения // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 30-35.
50. Остапенко Г. А., Колбасов С. М. Модели тактик реализации информационного конфликта // Информация и безопасность. 2006. Т. 9. № 1. С. 46-50.
51. Остапенко Г. А. Структурно-параметрическая модель информационного конфликта систем // Безопасность информационных технологий. 2007. № 2. С. 93-94.
52. Прилепский В. В. Конфликты в информационно-телекоммуникационных системах: учебное пособие. Часть 1. Воронеж: ВГУ. 2004. 145 с.
53. Толстых Н. Н., Павлов В. А., Воробьева Е. И. Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем: учебное пособие. – Воронеж: ВГУ. 2003. – 168 с.
54. Асосков А. Н., Малышева И. Н. К вопросу о синтезе алгоритма управления инфокоммуникационной системы в условиях информационного конфликта // Теория и техника радиосвязи. 2011. № 4. С. 19-26.
55. Мистров Л. Е. Основы обоснования критерия эффективности синтеза систем информационной безопасности для обеспечения конфликтной устойчивости взаимодействия социально-экономических организаций // Машиностроитель. 2014. № 10. С. 10-17.
56. Мистров Л. Е. Конфликтная устойчивость взаимодействия организационно-технических систем: общие понятия, научные подходы, метод синтеза // Научные технологии. 2011. Т. 12. № 9. С. 70-80.
57. Козирацкий Ю. Л., Ерофеев А. Н., Соколовский С. П. Модель конфликтного взаимодействия «нарушитель - подсистема защиты информации

автоматизированной системы управления» // Вестник Военного авиационного инженерного университета. 2012. № 1 (15). С. 210-217.

58. Ухин А. Л., Козирацкий Ю. Л. Вероятностная модель конфликта радиоэлектронных систем управления и телекоммуникации в условиях деструктивных воздействий // Системы управления и информационные технологии. 2014. Т. 57. № 3.2. С. 281-286.

59. Козирацкий Ю. Л., Кушев С. С., Чернухо И. И., Донцов А. А. Модель конфликтного взаимодействия систем управления противоборствующих сторон в условиях преднамеренных помех // Радиотехника. 2012. № 5. С. 56-61.

60. Будников С. А. Оценка вероятностных показателей в конфликте информационно-управляющих систем // Системы управления и информационные технологии. 2009. № 3(37). С. 27-31.

61. Жуматий В. П., Будников С. А., Паршин Н. В. Угрозы программно-математического воздействия. – Воронеж: ЦПКС ТЗИ, 2010. – 230 с.

62. Будников С. А., Соломатин М. С. Моделирование информационного конфликта систем на основе аппарата сетей Петри-Маркова // Наука и образование в XXI веке сборник научных трудов по материалам Международной научно-практической конференции. 2013. С. 20-22.

63. Бойко А. А., Будников С. А. Модель информационного конфликта специального программного средства и подсистемы защиты информации информационно технического средства // Радиотехника. 2015. № 4. С. 136-141.

64. Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статическими характеристиками // Радиотехника. 2013. № 7. С. 5-10.

65. Бойко А. А., Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3 (70). С. 84-92.

66. Вялых А. С., Вялых С. А., Сирота А. А. Оценка уязвимости информационной системы на основе ситуационной модели динамики конфликта // Информационные технологии. 2012. № 9. С. 15-21.

67. Вялых А. С., Вялых С. А., Сирота А. А. Алгоритм анализа надежности программного обеспечения информационных систем в условиях внутренних уязвимостей и негативных воздействий // Фундаментальные проблемы системной безопасности: материалы V Международной научной конференции. – М.: Вычислительный центр им. А.А. Дородницына. 2014. – С. 158-163.

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

69. Алферов А.Г., Толстых И.О., Толстых Н.Н., Поздышева О.В., Мордовин А.И. Устойчивость инфокоммуникационных систем в условиях информационного конфликта // Информация и безопасность. 2014. Т. 17. № 4. С. 558-567.

70. Стюгин М.А. Постановка задачи дезинформации в информационных системах // Информационные войны. 2014. № 3 (31). С. 6-11.
71. Стюгин М. А. Методика достижения информационного превосходства в конфликтных системах // Информационные войны. 2013. № 3 (27). С. 17-21.
72. Стюгин М. А. Рефлексивно-сигнатурный анализ конфликта // Искусственный интеллект и принятие решений. 2012. № 2. С. 39-50.
73. Стюгин М. А. Планирование действий в конфликте на уровне функциональных структур // Информационные войны. 2009. № 2. С. 16-21.
74. Шевцов В. А. Информационное противоборство как крайнее проявление конфликта в информационном пространстве // Радиотехника. 2001. № 3. С. 87-93.
75. Чукляев И. И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // Т-Comm: Телекоммуникации и транспорт. 2015. №2. С. 64-68.
76. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.
77. Якушенко С. А., Прасько Г. А., Дворовой М. О., Веркин С. С. К вопросу решения антагонистических задач при комплексном противодействии сторон // Научноёмкие технологии в космических исследованиях Земли. 2012. № 1. С. 24-26.
78. Данеев А. В., Воробьёв А. А., Лебедев Д. М. Исследование динамики поведения сложных организационно-технических систем в условиях воздействия неблагоприятных факторов // Вестник Воронежского института МВД России. 2010. № 2. С. 163-171.
79. Григорьев В. Р., Шуркин Л. О. Сетецентрические войны с позиции синергетики // Вестник Российского государственного гуманитарного университета. 2014. № 11. С. 67-100.
80. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.
81. Паршуткин А. В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.
82. Паршуткин А. В., Святкин С. А., Бажин Д. А., Сазыкин А. М. Радиоэлектронные информационные воздействия в конфликтах информационных и телекоммуникационных систем // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2015. № 5-6. С. 13-17.
83. Цвиркун А. Д. Основы синтеза структуры сложных систем. – М.: Наука, 1982. – 200 с.

84. Гуревич И. М. Многоуровневая модель сети связи // Вопросы кибернетики. Протоколы и методы коммутации в вычислительных сетях. 1986. С. 72-88.
85. Абраменков А. Н., Петухова Н. В., Фархадов М. П., Фрисов А. В., Гуревич И. М. Многоуровневые модели сетевых систем и комплекс программ расчета их статических и динамических характеристик // XII Всероссийское совещание по проблемам управления ВСПУ-2014. – М., 2014. – С. 7375-7386.
86. Агеев Д. В. Проектирование современных телекоммуникационных систем с использованием многоуровневых графов // Восточно-Европейский журнал передовых технологий. 2010. № 4/2 (46). С. 75-77.
87. Агеев Д. В. Моделирование современных телекоммуникационных систем многослойными графами // Проблемы телекоммуникаций. 2010. № 1 (1). С. 23-34. URL: http://pt.journal.kh.ua/2010/1/1/101_agey-ev_simulation.pdf (дата обращения 16.09.2015).
88. Илюхин А. А., Осипов А. Н. Алгоритм оптимизации ресурсов радиointерфейса спутниковых каналов обмена данными оперативно-диспетчерского управления // Информационные системы и технологии. 2014. № 4. С. 47–52.
89. Илюхин А. А., Щербаков М. В. Структурные и динамические свойства управления процессами обработки и передачи пакетных данных в мультисервисных спутниковых сетях // Т-Com. Телекоммуникации и транспорт. 2014. № 5. С. 28–32.
90. Маслобоев А. В., Путилов В. А., Сютин А. В. Координация в многоуровневых сетевых системах управления региональной безопасностью: подход и формальная модель // Научно-технический вестник информационных технологий, механики и оптики. 2015. Том 15. № 1. С. 130-138.
91. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. М.: СИНТЕГ, 1999. 232 с.
92. Гуревич И. М. Динамическая модель сети связи // Теория телетрафика в системах информатики. 1989. С. 77-86.
93. Гуревич И. М. Динамические свойства сетевых систем // Вопросы кибернетики. Архитектура и протоколы вычислительных сетей. 1990. С. 22-44.
94. Девянин П. Н. Модели безопасности компьютерных систем: учебное пособие для студентов вузов. – М.: Издательский центр «Академи», 2005. – 144 с.
96. Коцыняк М. А., Кулешов И. А., Лаута О. С. Устойчивость информационно-телекоммуникационных сетей. – СПб.: Издательство Политехнического университета, 2013. – 93 с.
97. Коцыняк М. А., Осадчий А. И., Коцыняк М. М., Лаута О. С., Дементьев В. Е., Васюков Д. Ю. Обеспечение устойчивости информационно-телекоммуникационных систем в условиях информационного противоборства. – СПб.: ЛО ЦНИИС, 2015. – 126 с.
98. Новиков Д. А. Механизмы функционирования многоуровневых организационных систем. – М.: Фонд "Проблемы управления", 1999. – 161 с.

99. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 344 с.
100. Месарович М., Такахара И. Общая теория систем: Математические основы. – М.: Мир, 1978. 311 с.
101. Калинин В. Н., Резников Б. А., Варакин Е. И. Теория систем и оптимального управления. Часть 1: Основные понятия, математические модели и методы анализа систем. – Л.: ВИКИ им. А.Ф. Можайского, 1979. – 319 с.
102. Калинин В. Н., Резников Б. А. Теория систем и управления (структурно-математический подход). – Л.: ВИКИ, 1987. – 417 с.
103. Дружинин В. В., Конторов Д. С. Вопросы военной системотехники. – М. Воениздат, 1976. – 224 с.
104. Вакуленко А. А., Шевчук В. И. Математическая модель динамики конфликта радиоэлектронных систем // Радиотехника. 2011. № 1. С. 56-59.
105. Маевский Ю. И. Основные положения методологии синтеза многофункциональной конфликтно-устойчивой системы радиоэлектронной борьбы // Радиотехника. 2010. № 6. С. 61-66.
106. Поповский В. В., Лемешко А. В., Евсеева О. Ю. Математические модели телекоммуникационных систем. Часть 1. Математические модели функциональных свойств телекоммуникационных систем // Проблемы телекоммуникаций. 2011. № 2 (4). С. 3-41.
107. Краснова С. А., Уткин В. А. Каскадный синтез наблюдателей состояния динамических систем. – М.: Наука, 2006. – 272 с.
108. Рубинштейн М. И. Оптимальная группировка взаимосвязанных объектов. Монография. – М.: Наука, 1989. – 168 с.
109. Гурин Л. С., Дымарский Я. С., Меркулов А. Д. Задачи и методы оптимального распределения ресурсов. – М.: Сов. радио, 1968. – 463 с.
110. Кини Р. Л., Райфа Х. Принятие решений при многих критериях, предпочтения и замещения. Пер. с англ. / Под ред. И.Ф. Шахнова. – М.: Радио и связь, 1981. – 560 с.
111. Угольницкий Г. А. Иерархическое управление устойчивым развитием. М.: Издательство физико-математической литературы, 2010. 336 с.
112. Усов А. Б. Борьба с коррупцией в динамических системах управления иерархической структуры // Известия Южного федерального университета. Технические науки. 2012. № 6 (131). С. 224-228.
113. Деттмер У. Теория ограничений Голдратта: Системный подход к непрерывному совершенствованию / Пер. с англ. 2-е изд. – М.: Альпина Бизнес Букс, 2008. – 444 с.

References

1. Budnikov S. A., Grevtsev A. I., Ivantsov A. V., Kil'diushhevskii V. M., Koziratskii A. Iu., Koziratskii Iu. L., Kushchev S. S., Lysikov V. F., Parinov M. L., Prokhorov D. V. *Modeli informatsionnogo konflikta sredstv poiska i obnaruzheniia. Monografiia* [Model information conflict of search and discovery. Treatise]. Moscow, Radiotekhnika Publ., 2013. 232 p. (in Russian).

2. Novikov D. A. Hierarchical models of combat. *Upravlenie bol'simi sistemami*, 2012, no. 37, pp. 25-62 (in Russian).
3. Vladimirov V. I., Vladimirov I. V. *Osnovy otsenki konfliktno-ustoichivyykh sostoianii organizatsionno-tekhnicheskikh sistem (v informatsionnykh konfliktakh)* [Basis of assessment of the conflict-stable States of organizational and technical systems (in information conflicts)]. Voronezh, Military aviation engineering University, 2008. 231 p. (in Russian).
4. Koziratskiy Ju. L., Podluzhnyi V. I., Parinov M. L. Metodicheskii podkhod k postroeniiu veroiatnostnoi modeli konflikta slozhnykh sistem [Methodical approach to constructing probabilistic models of complex conflict systems]. *Vestnik of Military Institute of Radioelectronics*, 2005, no. 3, pp. 4-16 (in Russian).
5. Ziuko A. G. *Pomekhoustoichivost' i effektivnost' sistem svyazi* [Noise immunity and efficiency of communication systems]. Moscow, Svyaz Publ., 1972. 359 p. (in Russian).
6. Maksimov M. V., Bobnev M. P., Krivitskii B. Kh., Gorgonov G. I., Stepanov B. M., Shustov L. N., Il'in V. A. *Zashchita ot radiopomekh* [Protection from radio interference]. Moscow, Sov. Radio Publ., 1976. 496 p. (in Russian).
7. Korzhik V. I., Fink M. M., Shchelkunov K. N. *Raschet pomekhoustoichivosti sistem peredachi diskretnoi informatsii* [The calculation of the noise immunity of systems of discrete information transmission]. Moscow, Radio i svyaz Publ., 1981. 267 p. (in Russian).
8. Tuzov G. I., Sivov V. A., Prytkov V. I. and etc. *Pomekhozashchishchennost' radiosistem so slozhnymi signalami* [Interference protection radio systems with complex signals]. Moscow, Radio i Svyaz Publ., 1985. 264 p. (in Russian).
9. Paliy A. I. *Radioelektronnaia bor'ba* [Electronic warfare]. Moscow, Voenizdat Publ., 1989. 350 p. (in Russian).
10. Perunov Ju. M., Matsukevich V. V., Vasil'ev A. A. *Zarubezhnye radioelektronnye sredstva. Tom 2: Sistemy radioelektronnoi bor'by* [Overseas Radio-Electronic Equipment. Tom 2: Electronic Warfare Systems]. Moscow, Radiotekhnika Publ., 2010. 352 p. (in Russian).
11. Radzievskiy V. G. and etc. *Sovremennaya radioelektronnaia bor'ba. Voprosy metodologii* [Modern electronic warfare. Methodological issues]. Moscow, Radiotekhnika Publ., 2006. 424 p. (in Russian).
12. Kuprijanov A. I., Saharov A. V. *Radioelektronnye sistemy v informatsionnom konflikte* [Radio-electronic systems in information conflict]. Moscow, Vuzovskaia Kniga Publ., 2003. 528 p. (in Russian).
13. Kuprijanov A. I., Shustov L. N. *Radioelektronnaia bor'ba. Osnovy teorii* [Electronic warfare. Fundamentals of the theory]. Moscow, Vuzovskaia Kniga Publ., 2011. 800 p. (in Russian).
14. Kuprijanov A. I. *Radioelektronnaia bor'ba* [Electronic warfare]. Moscow, Vuzovskaia Kniga Publ., 2013. 360 p. (in Russian).
15. Borisov V. I., Zinchuk V. M. *Pomekhozashchishchennost' sistem radiosvyazi. Veroiatnostno-vremennoi podkhod* [Noise immunity of radio communication systems. Probabilistic-temporal approach]. Moscow, Radio i Svyaz Publ., 1999. 252 p. (in Russian).

16. Borisov V. I., Zinchuk V. M., Limarev A. E., Nemchilov A. V., Chaplygin A. A. *Prostranstvennye i veroiatnostno-vremennye kharakteristiki effektivnosti stantsii otvetnykh pomekh pri podavlenii sistem radiosviazi* [Spatial and probabilistic-time characteristics of the effectiveness of the response stations interference suppression of radio communication systems]. Voronezh, Kontsern "Sozvezdie" Publ., 2007. 354 p. (in Russian).
17. Vladimirov V. I. *Printsipy i apparat sistemnykh issledovaniy radioelektronnogo konflikta* [The principles and apparatus of the electronic system studies conflict]. Voronezh, Voronezh Higher Military Engineering College of Radioelectronics, 1992. (in Russian).
18. Vladimirov V. I., Gal'ianov G. P. *Effektivnost' kompleksov REP i metody ee otsenki* [The efficiency of complexes of radio-electronic jamming and assessment methods]. Voronezh, Voronezh Higher Military Engineering College of Radioelectronics, 1993. (in Russian).
19. Vladimirov V. I., Gostev V. A. *Osnovy radiopodavleniya, postroeniya i primeneniya sredstv i kompleksov REP sistem peredachi informatsii. Tom 2.* [The basis of the countermeasure, the construction and application of funds and complexes radio-electronic suppression of information transmission systems]. Voronezh, Military Engineering College of Radioelectronics, 1997. (in Russian).
20. Vladimirov V. I. *Informatsionnye osnovy radiopodavleniya linii radiosviazi v dinamike radioelektronnogo konflikta* [Information basis of the countermeasure of radio communications in the dynamics of electronic conflict]. Voronezh, Military Engineering College of Radioelectronics, 2003. 276 p. (in Russian).
21. Vladimirov V. I., Likhachev V. P., Shliakhin V. M. *Antagonisticheskii konflikt radioelektronnykh sistem* [Antagonistic conflict radio-electronic systems]. Moscow, Radiotekhnika Publ., 2004. 384 p. (in Russian).
22. Semisoshenko M. A. *Upravlenie avtomatizirovannymi setiami dekametrovoi svyazi v usloviyakh slozhnoi radioelektronnoi obstanovki* [The management of the automated networks decameter communication in a complex electronic environment]. Saint-Petersburg, Military Communications Academy, 1997. 364 p. (in Russian).
23. Chudnov A. M. *Analiz pomekhozashchishchennosti linii i setei svyazi* [Analysis of noise immunity of lines and communication networks]. Leningrad, Military Communications Academy, 1988. 34 p. (in Russian).
24. Chudnov A. M. *Pomekhoustoichivost' linii i setei svyazi v usloviyakh optimizirovannykh pomekh* [Interference resistance lines and communication networks under conditions optimized interference]. Leningrad, Military Communications Academy, 1986. 84 p. (in Russian).
25. Barashkov P. N., Rodimov A. P., Tkachenko K. A., Chudnov A. M. *Model' sistemy svyazi s upravlyаемymi strukturami v konfliktnykh usloviyakh* [Model of communication system with controlled structures in conflict settings]. Leningrad, Military Communications Academy, 1986. 52 p. (in Russian).
26. Burachenko D. L. *Optimal'noe razdelenie tsifrovyykh signalov mnogikh pol'zovatelei v liniyakh i setiyakh svyazi v usloviyakh pomekh* [Optimal separation of digital signals of many users in lines and communication networks under

interference]. Leningrad, Military Communications Academy, 1990. 302 p. (in Russian).

27. Kuznetsov V. I. *Radiosviaz' v usloviakh radioelektronnoi bor'by* [Radio communication electronic warfare conditions]. Voronezh, Voronezh Research Institute of Communications, 2002, 403 p. (in Russian).

28. Bogovik A. V., Ignatov V. V. *Effektivnost' sistem voennoi svyazi i metody ee otsenki* [The effectiveness of military communications systems and assessment methods]. Saint-Petersburg, Military Communications Academy, 2006. 183 p. (in Russian).

29. Isakov E. E. *Ustoichivost' voennoi svyazi v usloviakh informatsionnogo protivoborstva* [The stability of military communications in the conditions of information warfare]. Saint-Petersburg, Peter the Great St.Petersburg Polytechnic University, 2009. 400 p. (in Russian).

30. Odоеvskiy S. M., Kaliuka V. I. *Adaptivno-igrovoe modelirovanie voennykh setei besprovodnogo abonentskogo dostupa* [Adaptive-game modeling of military networks broadband wireless access]. Tom 1. Novocherkassk, Educational-Production Center «Nabla», 2009. 216 p. (in Russian).

31. Nikolayev V. I., Fyodorov F. E. Digital Communication System Functioning under Radio Electronic Collision Condition from Minimax Position of the Game Theory (Part 1). *Teoriia i Tekhnika Radiosvazi*, 2010, no. 2, pp. 37-43 (in Russian).

32. Nikolayev V. I., Fyodorov F. E. Digital Communication System Functioning under Radio Electronic Collision Condition from Minimax Position of the Game Theory (Part 2). *Teoriia i Tekhnika Radiosvazi*, 2010, no. 2, pp. 44-49 (in Russian).

33. Shabalin E. A. Methods of radio communication systems' efficiency upgrading in warfare environments. *Telecommunications and Radio Engineering*, 2008, no. 9, pp. 40-44 (in Russian).

34. Shabalin E. A., Milov V. R. Network Resources Allocation with Information Value Consideration in Case of Electromagnetic Blanketing. *Informatsionno-izmeritelnye i upravlyayushchie systemy*, 2008, no. 11, pp. 87-93 (in Russian).

35. Radko N. M., Mokrousov A. N. Dynamic model of adaptive radiomeans to interferences with use of networks Petri. *Informatsiia i bezopasnost*, 2009, no. 2, pp. 257-262 (in Russian).

36. Maltcev G. N., Vozniuk V. V., Tuktamyshev M. R. Modelirovanie konflikta slozhnykh radio-tekhnicheskikh sistem metodom parallel'nykh razvivaiushchikhsia stokhasticheskikh protsessov [Modeling of complex conflict radio-technical systems by developing parallel stochastic processes]. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 5, pp. 26-33 (in Russian).

37. Radzievskii V. G., Sirota A. A. *Informatsionnoe obespechenie radioelektronnykh sistem v usloviakh konflikta* [Information support of electronic systems in conflict]. Moscow, IPRZR Publ., 2001. 456 p. (in Russian).

38. Starodubtsev Ju. I., Bukharin V. V., Semenov S. S. Tekhnosfernaia voina [Techno War]. *Military Thought*, 2012, no. 7. pp. 22-31 (in Russian).

39. Starodubtsev Ju. I., Bukharin V. V., Semenov S. S. Technospherny war. *Informatsionnye sistemy i tekhnologii*, 2011, no. 1, pp. 80-85 (in Russian).
40. Starodubtsev Ju. I., Bukharin V. V., Semenov S. S. Techno War. *Nauchno-informatsionnyi zhurnal Armiia i obshchestvo*, 2010, no. 4, pp. 6-11 (in Russian).
41. Semenov S. S., Gusev A. P., Barbotko N. V. Assessment Information the Combat Potential of the Parties in Technosphere Conflicts. *High Tech in Earth Space Research*, 2013, vol. 5, no. 6, pp. 10-21 (in Russian).
42. Novikov D. A., Chkhartishvili A. G. *Refleksivnye igry* [Reflexive games]. Moscow, SINTEG Publ., 2003. 149 p. (in Russian).
43. Novikov D. A., Chkhartishvili A. G. *Prikladnye modeli informatsionnogo upravleniia* [Reflexive grapelade model of information management]. Moscow, Institute of Control Sciences RAS, 2004. 129 p. (in Russian).
44. Novikov D. A. *Setevye struktury i organizatsionnye sistemy* [Network structure and organizational system]. Moscow, Institute of Control Sciences RAS, 2003. 102 p. (in Russian).
45. Gubanov D. A., Novikov D. A., Chkhartishvili A. G. *Sotsial'nye seti: modeli informatsionnogo vliianiia, upravleniia i protivoborstva* [Social networks: models of information influence, control and conflict]. Moscow, Izdatel'svo fiziko-matematicheskoi literatury Publ., 2010. 228 p. (in Russian).
46. Rastorguev S. P. *Matematicheskie modeli v informatsionnom protivoborstve. Ekzistentsial'naia matematika* [Mathematical models in information confrontation. Existential mathematics]. Moscow, Center for Strategic Assessment and Forecasts, 2014. 260 p. (in Russian).
47. Biryukov D. N., Rostovtsev Yu. G. Approach to creation of the consistent theory of synthesis scenarios of anticipatory behavior in the conflict. *Trudy SPIIRAN*, 2015, no. 1, pp. 94-111 (in Russian).
48. Biryukov D. N., Lomako A. G. Podkhod k postroeniiu IB-sistem, sposobnykh sintezirovat' stsennariu uprezhdaiushchego povedeniia v informatsionnom konflikte [An approach to building information security systems that are able to synthesize scenarios anticipatory behavior in information conflict]. *Zashchita informatsii. Insaid*, 2014, vol. 60, no. 6, pp. 42-49 (in Russian).
49. Biryukov D. N., Lomako A. G., Sabirov T. R. Multi-Level Preventive Behavior Scenario Modeling. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2014, no. 4, pp. 30-35 (in Russian).
50. Ostapenko G. A., Kolbasov S. M. Models of the Tactics of Realisation of the Informational Conflict. *Informatsiia i bezopasnost*, 2006, vol. 9, no. 1, pp. 46-50 (in Russian).
51. Ostapenko G. A. Strukturno-parametricheskaia model' informatsionnogo konflikta system [Structural-parametric model of the information conflict systems]. *Bezopasnost' informatsionnykh tekhnologii*, 2007, no. 2, pp. 93-94 (in Russian).
52. Prilepskiy V. V. *Konflikty v informatsionno-telekommunikatsionnykh sistemakh: uchebnoe posobie* [Conflicts in information and telecommunication systems]. Tom 1. Voronezh, Voronezh State University, 2004. 145 p. (in Russian).
53. Tolstykh N. N., Pavlov V. A., Vorobeva E. I. *Vvedenie v teoriuu konfliktnogo funktsionirovaniia informatsionnykh i informatsionno-upravliaiushchikh*

sistem [Introduction to the theory of conflict of functioning of the information and information management systems]. Voronezh, Voronezh State University, 2003. 168 p. (in Russian).

54. Asoskov A. N., Malysheva I. N. On infocommunication system management algorithm synthesis under information conflict conditions. *Teoriia i tekhnika radiosviazi*, 2011, no. 4, pp. 19-26 (in Russian).

55. Mistrov L. E. Osnovy obosnovaniia kriteriia effektivnosti sinteza sistem informatsionnoi bezopasnosti dlia obespecheniia konfliktnoi ustoichivosti vzaimodeistviia sotsial'no-ekonomicheskikh organizatsii [Rationale of criterion of efficiency of synthesis of systems of information security to ensure conflict stability of the interaction between socio-economic organizations]. *Mashinostroitel*, 2014, no. 10, pp. 10-17 (in Russian).

56. Mistrov L. E. Disputed stability of interaction organizational-technical systems: the general concepts, scientific approaches, synthesis method. *Naukoemkie tekhnologii*, 2011, vol. 12, no. 9, pp. 70-80 (in Russian).

57. Koziratsky Ju. L., Erofeev A. N., Sokolovskii S. P. Model' konfliktного vzaimodeistviia "narushitel - podсистема zashchity informatsii avtomatizirovannoi sistemy upravleniia" [Model of conflict interaction "violator - the subsystem of information security of automated control systems"]. *Vestnik Voennogo aviatsionnogo inzhenernogo universiteta*, 2012, vol. 15, no. 1, pp. 210-217 (in Russian).

58. Ukhin A. L., Koziratsky Ju. L. Veroiatnostnaia model' konflikta radioelektronnykh sistem upravleniia i telekommunikatsii v usloviakh destruktivnykh vozdeistvii [Probabilistic model of conflict radio-electronic control systems and telecommunications in terms of destructive impacts]. *Sistemy upravleniia i informatsionnye tekhnologii*, 2014, vol. 57. no. 3.2, pp. 281-286 (in Russian).

59. Koziratsky Ju. L., Kushev S. S., Chernuh I. I., Dontsov A. A. Model of disputed interaction of control systems of the contradictory parties in the conditions of deliberate hindrances. *Radiotekhnika*, 2012, no. 5, pp. 56-61 (in Russian).

60. Budnikov S. A. Estimation of likelihood parametres in the conflict of information control systems. *Sistemy upravleniia i informatsionnye tekhnologii*, 2009, vol. 37, no. 3, pp. 27-31 (in Russian).

61. Zhumatiy V. P., Budnikov S. A., Parshin N. V. *Ugrozy programmno-matematicheskogo vozdeistviia* [Threats software and mathematical exposure]. Voronezh, The center for training of specialists for technical protection of information, 2010. 230 p. (in Russian).

62. Budnikov S. A., Solomatin M. S. Modelirovanie informatsionnogo konflikta sistem na osnove apparata setei Petri-Markova [Modeling of information conflict of systems based on the formalism of Petri nets and Markov]. *Nauka i obrazovanie v XXI veke* [Conference on Science and Education in the XXI Century], 2013, pp. 20-22 (in Russian).

63. Boyko A. A., Budnikov S. A. Model of information conflict between special software and information security subsystem of information-technical tool. *Radiotekhnika*, 2015, no. 4, pp. 136-141 (in Russian).

64. Boyko A. A., Khramov V. U. Model of information conflict between special software and information-technical tools in military warfare with static characteristics. *Radiotekhnika*, 2013, no. 7, pp. 5-10 (in Russian).
65. Boyko A. A., Djakova A. V. Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools. *Informatsionno-upravliaiushchie sistemy*, 2014, vol. 70, no. 3, pp. 84-92 (in Russian).
66. Vyalykh A. S., Vyalykh S. A., Sirota A. A. Estimation of Vulnerability of the Information System at Purposeful Attacks of the Malefactor. *Informatsionnye tekhnologii*, 2012, no. 9, pp. 15-21 (in Russian).
67. Vyalykh A. S., Vyalykh S. A., Sirota A. A. Algoritm analiza nadezhnosti programmogo obespecheniia informatsionnykh sistem v usloviakh vnutrennikh uiazvimostei i negativnykh vozdествii [Algorithm analysis, software reliability of information systems in the context of internal vulnerabilities and negative impacts]. *Fundamental'nye problemy sistemnoi bezopasnosti* [Conference "Fundamental problems of system security"]. Moscow, Dorodnicyn Computing Centre of RAS, 2014, pp. 158-163 (in Russian).
68. Alferov A. G., Vlasov J. B., Tolstykh I. O., Tolstykh N. N., Chelajdinov J. V. The formalized representation of the evolving information conflict in telecommunication system. *Radiotekhnika*, 2012, no. 8. pp. 27-33 (in Russian).
69. Alferov A. G., Tolstykh I. O., Tolstykh N. N., Pozdysheva O. V., Mordovin A. I. Ustochivost' infokommunikatsionnykh sistem v usloviakh informatsionnogo konflikta [Sustainability of information and communication systems in terms of information conflict]. *Informatsiia i bezopasnost*, 2014, vol. 17, no. 4, pp. 558-567 (in Russian).
70. Styugin M. A. Statement of the problem of misinformation in information systems. *Informatsionnye voiny*, 2014, vol. 31, no. 3, pp. 6-11 (in Russian).
71. Styugin M. A. Methods to achieve information superiority in conflict systems. *Informatsionnye voiny*, 2013, vol. 27, no. 3, pp. 17-21 (in Russian).
72. Styugin M. A. The is reflexive-signature analysis of conflicts. *Scientific and Technical Information Processing*, 2012, no. 2, pp. 39-50 (in Russian).
73. Styugin M. A. Action planning in the conflict at functional structure level. *Informatsionnye voiny*, 2009, no. 2, pp. 16-21 (in Russian).
74. Shevtsov V. A. Informatsionnoe protivoborstvo kak krainee proiavlenie konflikta v informatsionnom prostranstve [Information confrontation as a manifestation of the conflict in the information space]. *Radiotekhnika*, 2001, no. 3, pp. 87-93 (in Russian).
75. Chuklyaev I. I. Game model justification means of complex protection of information resources on hierarchical information and control system. *T-Comm*, 2015, no. 2, pp. 64-68 (in Russian).
76. Makarenko S. I., Chuklyaev I. I. The terminological basis of the informational conflict area. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 13-21 (in Russian).

77. Yakushenko S. A., Prasko G. A., Dvorovoy M. O., Verkin S. S. Solution of antagonistic tasks in case of complex counteraction of the sides. *High technologies in Earth space research*, 2012, no. 1, pp. 24-26 (in Russian).

78. Daneev A. V., Vorobev A. A., Lebedev D. M. Investigation of dynamics of behaviour of complex organizing technical systems in condition of the influence of disadvantage factors. *Vestnik Voronezhskogo instituta MVD Rossii*, 2010, no. 2, pp. 163-171 (in Russian).

79. Grigorev V. R., Shurkin L. O. Setetsentricheskie voyny s pozitsii sinergetiki [Setetsentricheskie voyny with pozitsii sinergetiki]. *Vestnik Rossiiskogo gosudarstvennogo gumanitarnogo universiteta*, 2014, no. 11, pp. 67-100 (in Russian).

80. Antonovich P. I., Makarenko S. I., Mihaylov R. L., Ushanov K. V. New means of destructive effects on network centric military command, control and communication systems in the information space. *Vestnik Akademii voennykh nauk*. 2014, vol. 48, no. 3, pp. 93-101 (in Russian).

81. Parshutkin A. V. Conceptual interconnection model of conflict information and telecommunication systems. *Voprosy kiberbezopasnosti*, 2014, vol. 8, no. 5, pp. 2-6 (in Russian).

82. Parshutkin A. V., Svyatkin S. A., Bazhin D. A., Sazykin A. M. Radio-electronic information influences in the conflicts of information and telecommunication systems. *Voprosy oboronnoi tekhniki. 16-th Seriya*, 2015, no. 5-6, pp. 13-17 (in Russian).

83. Tvircun A. D. *Fundamentals of synthesis of structure of complex systems*. Moscow, Nauka Publ., 1982. 200 p. (in Russian).

84. Gurevich I. M. Mnogourovnevaia model' seti svyazi [Multi-level model of the communication network]. *Voprosy kibernetiki. Protokoly i metody kommutatsii v vychislitel'nykh setiakh*, 1986, pp. 72-88 (in Russian).

85. Abramnikov A. N., Petukhova N. V., Farkhadov M. P., Frisov A. V., Gurevich I. M. Mnogourovnevye modeli setevykh sistem i kompleks programm rascheta ikh staticheskikh i dinamicheskikh kharakteristik [Multi-level models of network systems and the complex of programs of calculation of their static and dynamic characteristics]. *XII Vserossiiskoe soveshchanie po problemam upravleniia "VSPU-2014"* [XII all-Russia meeting on problems of management]. Moscow, 2014. pp. 7375-7386 (in Russian).

86. Ageev D. V. Proektirovanie sovremennykh telekommunikatsionnykh sistem s ispol'zovaniem mnogourovnevnykh grafov [The design of modern telecommunication systems using multi-level graphs]. *Vostochno-Evropeiskii zhurnal peredovykh tekhnologii*, 2010, vol. 46, no. 4/2, pp. 75-77 (in Russian).

87. Ageev D. V. Modelirovanie sovremennykh telekommunikatsionnykh sistem mnogosloinymi grafami [Modeling of telecommunication systems layered graphs]. *Problemi telekomunikatsii*, 2010, vol. 1, no. 1, pp. 23-34. Available at: http://pt.journal.kh.ua/2010/1/1/101_agey-ev_simulation.pdf (in Russian).

88. Iliukhin A. A., Osipov A. N. Algoritm optimizatsii resursov radiointerfeisa sputnikovykh kanalov obmena dannymi operativno-dispatcherskogo upravleniia [The algorithm of optimization of resources of the radio interface of the satellite

communication channels operatively-dispatching management]. *Informatsionnye sistemy i tekhnologii*, 2014, no. 4, pp. 47-52 (in Russian).

89. Iliukhin A. A., Shcherbakov M. V. Strukturnye i dinamicheskie svoistva upravleniia protsessami obrabotki i peredachi paketnykh dannykh v mul'tiservisnykh sputnikovykh setiakh [Structural and dynamic properties of the process control processing and transmission of packet data in a multiservice satellite networks]. *T-Com*, 2014, no. 5, pp. 28-32 (in Russian).

90. Masloboev A. V., Putilov V. A., Sioutine A. V. Coordination in multilevel network-centric control systems of regional security: approach and formal model. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2015, vol. 15, no. 1, pp. 130-138 (in Russian).

91. Griniaev S. N. *Intellektual'noe protivodeistvie informatsionnomu oruzhiu* [Intellectual opposition to arms information]. Moscow, SINTEG Publ., 1999. 232 p. (in Russian).

92. Gurevich I. M. Dinamicheskaya model' seti svyazi [The dynamic model of the communication network]. *Teoriia teletrafika v sistemakh informatiki*, 1989, pp. 77-86 (in Russian).

93. Gurevich I. M. Dinamicheskie svoistva setevykh sistem [Dynamic properties of network systems]. *Voprosy kibernetiki. Arkhitektura i protokoly vychislitel'nykh setei*, 1990, pp. 22-44 (in Russian).

95. Devianin P. N. *Modeli bezopasnosti komp'yuternykh sistem* [Models for computer security]. Moscow, Publishing center «Akademia», 2005. 144 p. (in Russian).

96. Kotsyniak M. A., Kuleshov I. A., Laut O. S. *Ustoichivost' informatsionno-telekommunikatsionnykh setei* [The stability of information-telecommunication networks]. Saint-Petersburg, Peter the Great St.Petersburg Polytechnic University, 2013. 93 p. (in Russian).

97. Kotsyniak M. A., Osadchiy A. I., Kotsyniak M. M., Laut O. S., Dement'ev V. E., Vasiukov D. Ju. *Obespechenie ustoichivosti informatsionno-telekommunikatsionnykh sistem v usloviakh informatsionnogo protivoborstva* [Sustainability Information and Telecommunication Systems in Terms of Information Warfare]. Saint-Petersburg, Saint-Petersburg Branch "Leningrad Branch of Central Science Research Telecommunication Institute", 2015. 126 p. (in Russian).

98. Novikov D. A. *Mekhanizmy funktsionirovaniia mnogourovnevnykh organizatsionnykh sistem* [Mechanisms of functioning of multilevel organizational systems]. Moscow, Fond "Problemy upravleniia" Publ., 1999. 161 p. (in Russian).

99. Mesarovic M. D., Macko D., Takahara Y. *Theory of multilevel hierarchical systems*. New York, Academic. 1970.

100. Mesarovic M. D. Takahara Y. *General systems theory: mathematical foundations*. New York, Academic press, 1975.

101. Kalinin V. N., Reznikov B. A., Varakin E. I. *Teoriia sistem i optimal'nogo upravleniia. Chast 1: Osnovnye poniatia, matematicheskie modeli i metody analiza sistem* [Systems theory and optimal control. Part 1: Basic concepts, mathematical models and methods of systems analysis]. Leningrad, Mozhaisky Military Space Institute, 1979. 319 p. (in Russian).

102. Kalinin V. N., Reznikov B. A. *Teoriia sistem i upravleniia (strukturno-matematicheskii podkhod)* [Systems theory and management (structural-mathematical approach)]. Leningrad, Mozhaitsky Military Space Institute, 1987. 417 p. (in Russian).
103. Druzhinin V. V., Kontorov D. S. *Voprosy voennoi sistemotekhniki* [The questions of military engineering]. Moscow, Voenizdat Publ., 1976. 224 p. (in Russian).
104. Vakulenko A. A., Shevchuk V. I. Matematicheskaya model' dinamiki konflikta radioelektronnykh sistem [A mathematical model of the dynamics of conflict radio-electronic systems]. *Radiotekhnika*, 2011, no. 1, pp. 56-59 (in Russian).
105. Maevskiy Ju. I. Osnovnye polozheniia metodologii sinteza mnogofunktsional'noi konfliktno-ustoichivoi sistemy radioelektronnoi bor'by [The main provisions of the methodology of synthesis of multi-functional conflict-a sustainable system of electronic warfare]. *Radiotekhnika*, 2010, no. 6, pp. 61-66 (in Russian).
106. Popovskiy V. V., Lemeshko A. V., Evseeva O. Ju. Matematicheskie modeli telekommunikatsionnykh sistem. Chast' 1. Matematicheskie modeli funktsional'nykh svoystv telekommunikatsionnykh sistem [Mathematical models of telecommunication systems. Part 1. The mathematical model of the functional properties of telecommunication systems]. *Problemy telekommunikatsii*, 2011, vol. 4, no. 2, pp. 3-41 (in Russian).
107. Krasnova S. A., Utkin V. A. *Kaskadnyi sintez nabliudatelei sostoiianiia dinamicheskikh sistem* [Cascade synthesis of observers for dynamic systems]. Moscow, Nauka Publ., 2006. 272 p. (in Russian).
108. Rubinshtein M. I. *Optimal'naya gruppировка vzaimosviazannykh obektov* [Optimal grouping of related objects]. Moscow, Nauka Publ., 1989. 168 p. (in Russian).
109. Gurin L. S., Dymarskii Ia. S., Merkulov A. D. *Zadachi i metody optimal'nogo raspredeleniia resursov* [Tasks and methods of optimal allocation of resources]. Moscow, Sov. Radio Publ., 1968. 463 p. (in Russian).
110. Keeney R. L., Raiff H. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. John Wiley & Sons Publ., 1976.
111. Ugol'nitskiy G. A. *Ierarkhicheskoe upravlenie ustoichivym razvitiem* [Hierarchical control of sustainable development]. Moscow, Fiziko-Matematicheskoi Literaturny Publ., 2010. 336 p. (in Russian).
112. Usov A. B. The Differential Model of Economic Corruption. *Izvestiia Iuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*, 2012, vol. 131, no. 6, pp. 224-228 (in Russian).
113. Dettmer H. W. *Goldratt's theory of constraints: a systems approach to continuous improvement*. ASQ Quality Press, 1997.

Статья поступила 17 сентября 2015 г.

Информация об авторе

Макаренко Сергей Иванович – кандидат технических наук, доцент. Доцент кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: устойчивость сетей и систем связи к преднамеренным дестабилизирующим воздействиям; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: Россия, 197198, г. Санкт-Петербург, ул. Ждановская д. 13.

Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression

Makarenko S. I.

Statement of the problem: the means of information attacks on communication systems are actively developing now do actual development of scientific methods for modeling the effects of such attacks. We propose to use the concept of "information conflict" to describe the functioning of the communication system in terms of information attacks. We conducted an analysis which showed that the creation of new means of information attacks is done by the integration means of electronic warfare, information impacts, means of radio monitoring and computer reconnaissance. Multilevel dynamic model of information conflict takes into account the impact of these funds at different levels of the OSI model (Open System Interconnection Reference Model). **Purpose.** The aim of this work is to develop a dynamic model of information conflict communication system with the information attack system. We consider a communication system as complex multilevel hierarchical system. Information conflict of the communications system is considered as a set of local conflict situations for each level of the OSI model. **Used methods.** We analyzed models of conflict on the basis of the theory of games, theory of Markov processes, theory of Petri nets, theory of active management and substantiated the theory of dynamical systems as a basis for modeling the information conflict. **Novelty.** The functional relationships between elements of a communication system which exist at the same level or at different levels of the OSI, and representation of communication system in the form of a complex hierarchical structure in the model information of the conflict are the novelty of this model. Proved the principal possibility of developing new classes of attacks that focus on the creation and development of internal contradictions between different protocols, communications systems, and development of new multilevel attacks, which are implemented at various levels of the OSI model. **The results and their significance.** The model of information conflict in the communication system can be used to develop new strategies to manage communication in terms of information attacks. Additionally, this model can be used to justify new types of attacks, wich implementing a hidden functional suppression of the communications system through the establishment and development of the internal contradictions between its separate protocols.

Keywords: dynamic model, communication system, hierarchical system, complex system, information attack, information conflict, electronic warfare, information struggle, OSI model.

Information about Author

Makarenko Sergey Ivanovich – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. Mozhaisky Military Space Academy. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197198, Saint-Petersburg, Zhdanovskaya ulica, 13.

УДК 004.056

Анализ быстродействия алгоритмов вычисления секретного ключа в асимметричной криптосистеме RSA

Алексеев А. П., Дикарева К. Н., Макаров М. И.

Постановка задачи: при расчёте секретного ключа в криптосистеме RSA используется обобщённый алгоритм Евклида. В статье проводится сопоставление быстродействия обобщённого алгоритма Евклида с алгоритмами ALGO 1 и ALGO 2, разработанными авторами. **Целью работы** является проведение сравнительного анализа быстродействия трёх алгоритмов вычисления секретной экспоненты в криптосистеме RSA. Программная реализация алгоритмов осуществлена с помощью трёх систем программирования: Mathcad, Pascal и C#, что позволяет ослабить влияние среды программирования на полученные результаты. **Используемые методы:** сравнительный анализ быстродействия трёх алгоритмов выполнен экспериментальным методом путём измерения времени счёта при различных исходных данных. Вывод расчётных соотношений при разработке алгоритма ALGO 1 выполнен аналитически. Обоснование алгоритма ALGO 2 сделано путём доказательства пяти лемм. **Новизна:** разработано два новых алгоритма вычисления секретных экспонент. **Результат:** расчётным путём показано, что по убыванию быстродействия рассмотренные алгоритмы расположились так: обобщённый алгоритм Евклида, ALGO 1, ALGO 2. Выявлены причины различия в быстродействии рассмотренных алгоритмов. **Практическая значимость:** полученные результаты наглядно показали, как эффективность решения одной и той же задачи зависит от способа её решения. Три рассмотренных алгоритма проиллюстрированы программами на языках программирования Mathcad, Pascal и C#, а также примерами ручных расчётов. Это позволяет использовать результаты не только в научных целях, но и в учебном процессе.

Ключевые слова: асимметричная криптосистема RSA, алгоритм Евклида, быстродействие, секретный ключ, открытый ключ, экспонента, функция Эйлера, лемма, языки программирования.

Актуальность

Асимметричная криптосистема RSA используется для передачи ключей к симметричным криптосистемам, формирования цифровой подписи ответственных документов, создания почтовых клиентов [1, 2, 3]. Выбор значения открытой экспоненты влияет на характеристики криптосистемы. С одной стороны, уменьшение её значения (например, до 3) повышает скорость шифрования. С другой стороны, малые значения открытой экспоненты позволяют произвести успешную атаку на криптосистему [4]. Кроме того, значение открытой экспоненты влияет на время вычисления секретной экспоненты. Представляет интерес сделать попытку усовершенствовать широко используемый обобщённый алгоритм Евклида, который применяется при расчёте секретной экспоненты.

Постановка задачи

При расчёте секретной экспоненты в криптосистеме RSA используется обобщённый алгоритм Евклида. В статье производится сопоставление быстродействия обобщённого алгоритма Евклида с двумя алгоритмами ALGO 1 и ALGO 2, которые разработаны авторами. Оценка быстродействия алгоритмов может быть осуществлена аналитически или экспериментально [5]. В данной работе выбран второй путь.

Теоретическое обоснование

Расчёт секретной экспоненты t в криптосистеме RSA осуществляется с помощью сравнения [6]:

$$s \cdot t \equiv 1(\text{mod}(\varphi(r))), \quad (1)$$

здесь s – число взаимно простое с $\varphi(r)$, так называемая открытая экспонента; r – произведение двух простых чисел p и q (модуль); $\varphi(r)$ – функция Эйлера, которая вычисляется по формуле:

$$\varphi(r) = (p-1) \cdot (q-1). \quad (2)$$

Из сравнения (1) по вычисленному значению функции Эйлера $\varphi(r)$ и выбранному значению s требуется найти такое значение t , при котором целочисленное деление величины $s \cdot t$ на $\varphi(r)$ даст остаток 1.

Вычисление секретной экспоненты t ведётся, как правило, с помощью обобщённого алгоритма Евклида [1, 2], блок-схема которого показана на рис. 1.

Основная идея вычислений состоит в том, что вводятся два числа $\varphi(r)$ и s . Большее число делится на меньшее. Если остаток от деления равен нулю, то вычисления завершаются. В противном случае большее число заменяется остатком от деления, а затем деление циклически продолжается.

На блок-схеме алгоритма операция округления до меньшего целого числа обозначена прямыми скобками, операция нахождения остатка от целочисленного деления – аббревиатурой mod.

Тексты программ для реализации обобщённого алгоритма Евклида на языке математической системы Mathcad 15, языках программирования Pascal и C# приведены в Приложениях 1, 2, 3.

Обобщённый алгоритм Евклида предназначен для решения численным методом уравнения вида:

$$ax + by = \text{gcd}(a, b), \quad (3)$$

в котором известны два целых положительных числа a и b , а требуется найти целые числа x , y и наибольший общий делитель чисел $\text{gcd}(a, b)$, которые удовлетворяют указанному уравнению. Англоязычная аббревиатура gcd означает: greatest common divisor. В русскоязычной литературе часто используется аббревиатура НОД – наибольший общий делитель.

Пример 1.

Выполним ручной расчёт секретной экспоненты по обобщённому алгоритму Евклида. Результаты расчётов представлены в таблице 1. Согласно обобщённому алгоритму Евклида вычисления нужно завершить при $T_1=0$ (см. рис. 1). Результаты содержатся в переменных $T_2 \rightarrow x$ и $T_3 \rightarrow y$ на предпоследней итерации. Переменная T_1 на предпоследней итерации содержит значение остатка от целочисленного деления. Переменная P сохраняет значение T_3 на предыдущей итерации.

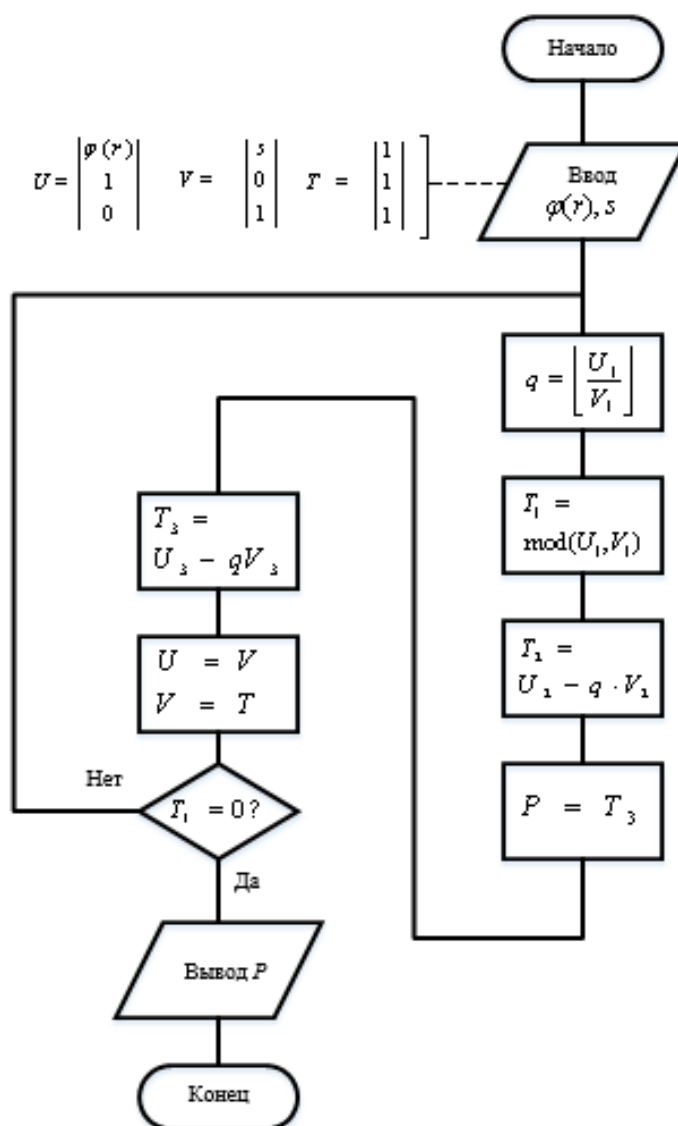


Рис. 1. Обобщённый алгоритм Евклида

Решение.

Исходные числа:

$\phi(r) = 460, s = 257$.

Таблица 1. Расчёт с помощью обобщённого алгоритма Евклида

Итерация	q	T_1	T_2	T_3	P
1	1	203	1	-1	1
2	1	54	-1	2	-1
...	...	...	...	...	...
6	6	1	-119	213	-34
7	2	0	257	-460	213

В результате расчётов получено: $x = -119, y = 213$.

Для проверки полученных результатов подставим найденные числа в уравнение (3):

$$460 \cdot (-119) + 257 \cdot 213 = -54740 + 54741 = 1.$$

Наибольший общий делитель чисел 460 и 257 должен быть равен 1. Это определяется правилом выбора открытой экспоненты [1]. Проверка показала, что числа -119 и 213 вычислены верно. Секретная экспонента равна 213, а остаток от целочисленного деления равен 1.

Рассмотрим ещё один алгоритм вычисления секретной экспоненты ALGO 1. Из сравнения (1) нужно найти такое целое число t , которое при целочисленном делении числа $m=s \cdot t$ на $\varphi(r)$ даст остаток, равный единице. Таким образом, число m должно быть обязательно больше числа $\varphi(r)$ хотя бы на единицу (так как остаток от целочисленного деления равен 1). Кроме того, число $m=\varphi(r)+1$ должно нацело делиться на число s , поэтому нужно проверять является ли целым число $k=m/s$. Если на первой итерации число k не является целым, то следует взять новое число $m=2\varphi(r)+1$, проверить является ли целым новое число $k=m/s$ и т.д., то есть с каждой новой итерацией число m должно увеличиваться на величину $\varphi(r)$.

Блок-схема алгоритма ALGO 1 показана на рис.2.

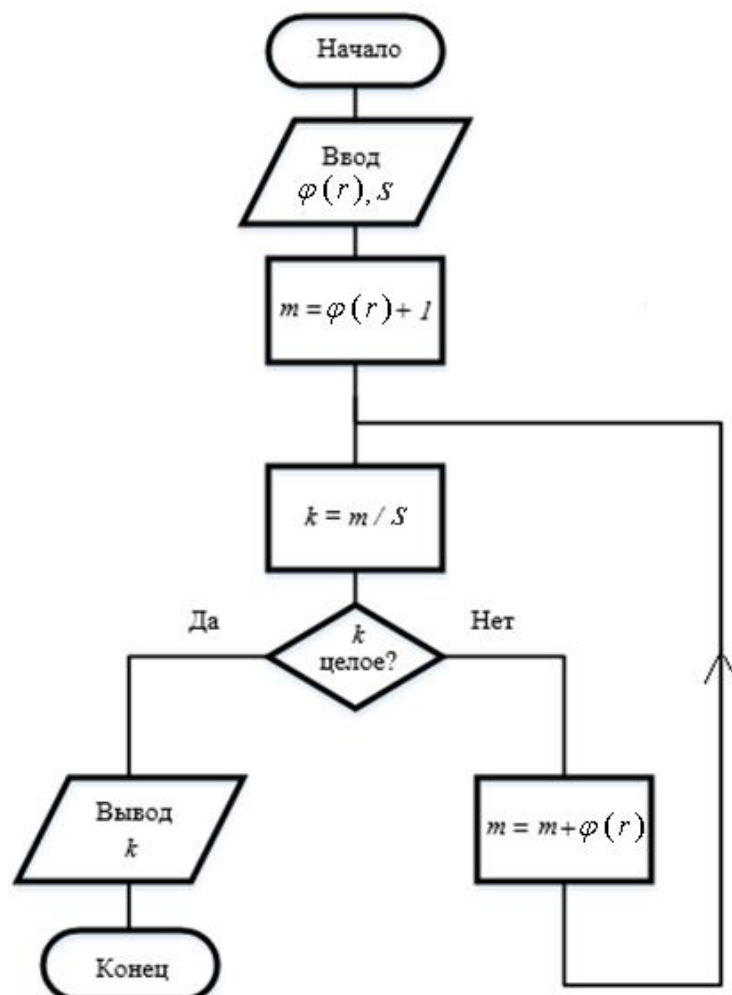


Рис. 2. Блок-схема алгоритма ALGO 1

В соответствии с алгоритмом ALGO 1 секретную экспоненту можно рассчитать по формуле:

$$t = \frac{n \cdot \varphi(r) + 1}{s}.$$

Здесь n определяет число необходимых итераций. Число n следует увеличивать от 1 до такого значения, при котором t станет целым числом. Из формулы видно, что число итераций n будет всегда меньше значения открытой экспоненты s .

Пример 2.

Выполним ручной расчёт с помощью алгоритма ALGO 1.

Решение.

Исходные числа: $s = 27$, $\varphi(r) = 460$.

Результаты расчётов помещены в таблицу 2.

Таблица 2. Расчёт с помощью алгоритма ALGO 1

Итерация	m	k	k целое ?	Экспонента
1	461	17,04	Нет	-
2	921	34,11	Нет	-
...	...	...	...	...
26	11961	443	Да	443

Секретная экспонента равна 443.

В Приложениях 4, 5 и 6 приведены программы для реализации алгоритма ALGO 1 на языке математической системы Mathcad 15, языках Pascal и C#.

Рассмотрим третий алгоритм нахождения секретной экспоненты (ALGO 2). Требование (1) можно записать иначе $s \cdot t - 1 = 0 \pmod{\varphi(r)}$, то есть целочисленное деление величины $s \cdot t - 1$ на $\varphi(r)$ должно дать остаток 0.

Требование к выбору секретного ключа t можно сформулировать так:

$$\frac{s \cdot t - 1}{\varphi(r)} = n, \quad (4)$$

где n – целое число.

Поиск числа t , удовлетворяющего соотношению (4), нужно вести среди чисел:

$$t \geq \frac{\varphi(r) + 1}{s}. \quad (5)$$

Обоснуем разработку алгоритма ALGO 2 с помощью лемм.

Лемма 1

Если $\varphi(r)$ кратно 10, а число s заканчивается цифрой 7, то число t должно заканчиваться цифрой 3.

Доказательство

Так как произведение указанных чисел s и t будет заканчиваться единицей, то в соответствии с (4) в результате вычитания единицы из произведения $s \cdot t$ будет получено число, кратное 10.

Таким образом, величину t нужно искать среди чисел, у которых последняя цифра 3, например, 3, 13, 23, 33, 43 и т.д.

Пример 3.

Пусть $\varphi(r) = 460$, $s = 27$, тогда в соответствии с (5) ответ нужно искать среди чисел больших 16,33, причём число $27 \cdot t - 1$ должно нацело делиться на число 460. Первое значение числа t , с которого следует начинать поиск числа, удовлетворяющего соотношениям (4) и (5), равно 23.

Результаты расчётов приведены в таблице 3.

Таблица 3. Расчёт с помощью алгоритма ALGO 2

Итерация	t	n	n целое?	Экспонента
1	23	17,04	Нет	-
2	33	34,11	Нет	-
3	43	51,148	Нет	-
...	...	...	...	...
43	443	443	Да	443

Расчёт секретного ключа после сорока трёх итераций дал значение 443. Как видно из таблицы, вычисления ведутся до тех пор, пока число n не станет целым.

Лемма 2

Если число $\varphi(r)$ кратно 10, а число s заканчивается цифрой 3, то число t должно заканчиваться цифрой 7.

Доказательство

Доказательство аналогично доказательству леммы 1.

Таким образом, величину t нужно искать среди чисел, заканчивающихся на цифру 7, например, 7, 17, 27, 37, 47 и т.д.

Пример 4.

Пусть $\varphi(r)=460$, $s=3$, тогда в соответствии с (4) ответ нужно искать среди чисел больших, чем 153,67, причём число $3 \cdot t - 1$ должно нацело делиться на $\varphi(r)$. Первое значение числа t , с которого следует начинать поиск числа, удовлетворяющего соотношениям (4) и (5), равно 157. Поиск секретного ключа в этом случае дал значение 307.

Лемма 3

Если $\varphi(r)$ кратно 10, а s заканчивается цифрой 9, то последняя цифра числа t должна быть 9.

Доказательство

Только произведение двух чисел, оканчивающихся цифрами 9 (при s , заканчивающимся на 9), даёт число, у которого последняя цифра 1. В этих случаях число $s \cdot t - 1$ будет кратно 10.

Пример 5.

Пусть $\varphi(r)=120$, $s=19$.

В соответствии с (5) поиск чисел t нужно вести среди целых чисел, которые больше 6,368. Число 9 не удовлетворяет условию (4), а число $t=19$ является искомым ответом.

Лемма 4

Если $\varphi(r)$ кратно 10, а s заканчивается цифрой 1, то последняя цифра числа t должна быть 1.

Доказательство

Только произведение двух чисел, оканчивающихся цифрами 1(при числе s , заканчивающемся цифрой 1), даёт число, у которого последняя цифра 1. В этих случаях число $s \cdot t-1$ будет кратно 10.

Пример 6.

Пусть $\varphi(r)=120$, $s=31$.

В соответствии с (5) поиск чисел t нужно вести среди целых чисел, которые больше 3,903.

Числа 11 и 21 не удовлетворяет условию (4), а число $t=31$ является ответом.

Лемма 5

Если $\varphi(r)$ кратно 10, то число s не может оканчиваться на цифру 5.

Доказательство

Числа $\varphi(r)$ и s должны быть взаимно простыми. Таким образом, при $\varphi(r)$, кратном десяти, число s может заканчиваться только цифрами 1, 3, 7 и 9.

Блок-схема алгоритма ALGO 2 показана на следующем рисунке.

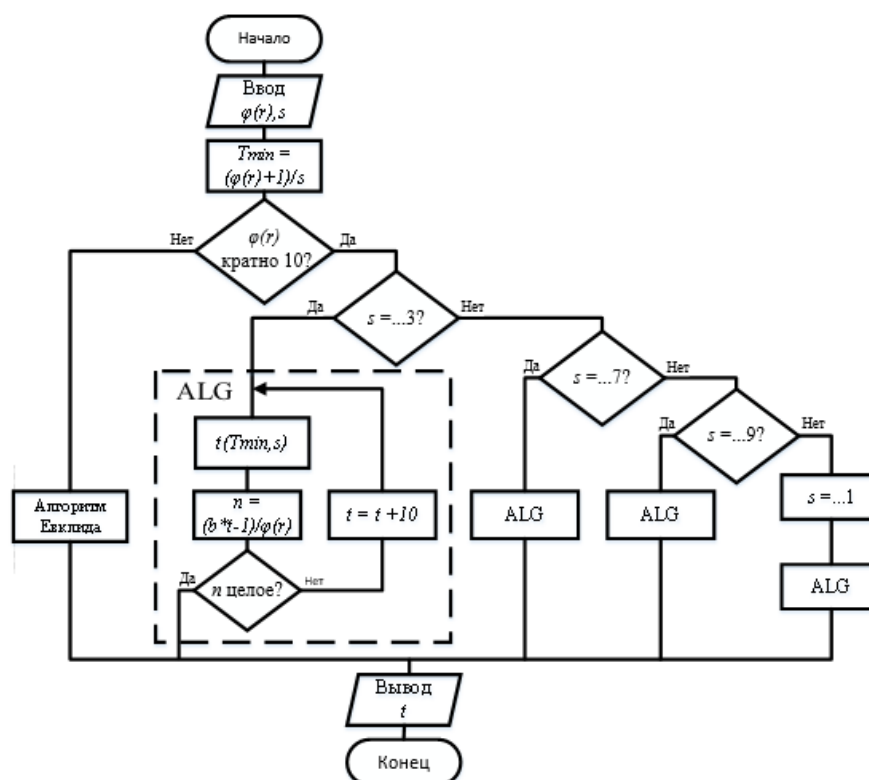


Рис. 3. Блок-схема алгоритма ALGO 2

В Приложении 7 приведён текст программы на языке математической системы Mathcad 15, а в Приложениях 8 и 9 – программы соответственно на языках программирования Pascal и C#.

Величина T_{min} вычисляется по формуле (5) и определяет наименьшее значение секретной экспоненты.

Работу алгоритма ALGO 2 можно описать так. Отличия этого алгоритма от обобщённого алгоритма Евклида существуют только при значениях функции Эйлера, кратных десяти. В этих случаях проводится анализ выбранной открытой экспоненты. Если она оканчивается цифрой 3, то секретный ключ должен оканчиваться цифрой 7. Приближение к искомой секретной экспоненте в этом алгоритме происходит путём многократного прибавления числа 10 к некоторому начальному числу (5). Если открытая экспонента оканчивается числом 7 (или 1, 9), то секретная экспонента должна оканчиваться цифрой 3 (соответственно 1, 9). В любом случае приращения равны 10.

Обсуждение результатов расчёта

Разработанные программы были использованы для оценки времени счёта секретной экспоненты по трём алгоритмам. Предварительные расчёты проводились на трёх ЭВМ, в трёх различных программных средах: Mathcad, Pascal и C#. Таблицы с фрагментами расчётов приведены в Приложениях 10, 11 и 12. Даже беглый анализ таблиц, приведённых в Приложениях 10, 11 и 12, показывает, что алгоритм ALGO 2 не может конкурировать по быстродействию с обобщённым алгоритмом Евклида и алгоритмом ALGO 1.

Для определения времени выполнения расчётов в программах на языке программирования C# применялся экземпляр класса Stopwatch, входящий в состав области имён System.Diagnostics. Запуск отсчёта времени выполнения программы осуществлялся методом StartNew, а по завершению счёта использовался метод ElapsedMilliseconds, возвращающий значение затраченного времени, выраженного в миллисекундах.

Чаще всего программы выполнялись за время менее одной миллисекунды. По этой причине в программах использовалось многократное циклическое повторение расчётов от 1000 до 2 000 000 раз. Программы были реализованы в виде консольных приложений. Однако время выполнения операций ввода-вывода через консоль не добавлялось ко времени, затраченному на вычисления.

Перечислим технические характеристики использованных вычислительных средств. При расчётах на Mathcad 15 использовался компьютер Asus R2N, с тактовой частотой 1 ГГц, объёмом ОЗУ 2 Гбайт (операционная система Windows XP). При вычислениях на языке программирования PascalABC.NET версия 2.2, сборка 1013 (17.08.2015) использовался компьютер Asus, с тактовой частотой 3,4 ГГц, объёмом ОЗУ 4 Гбайт. Расчёты на C# 4.0 велись на ЭВМ Lenovo ThinkCentre, с тактовой частотой 1.8 ГГц, объёмом ОЗУ 4 Гбайт (операционная система Windows 7). Программа была реализована в среде разработки Visual Studio 2010.

Более детальный анализ проведём с помощью рисунков, которые получены путём аппроксимации большого массива экспериментальных данных. Аппроксимация осуществлялась с помощью программы ТС 3D [7].

На рисунках 4 и 5 показаны зависимости времени t расчёта секретной экспоненты от значений открытой экспоненты s и функции Эйлера $\phi(r)$ для программ, составленных на языках программирования C# и Pascal (обобщённый алгоритм Евклида). Время на графиках выражено в микросекундах.

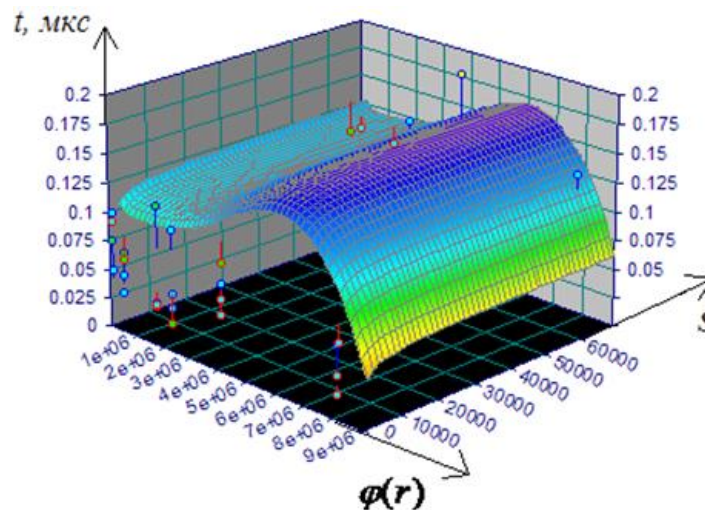


Рис. 4. Зависимость $t=F(s, \phi(r))$ для обобщённого алгоритма Евклида (C#)

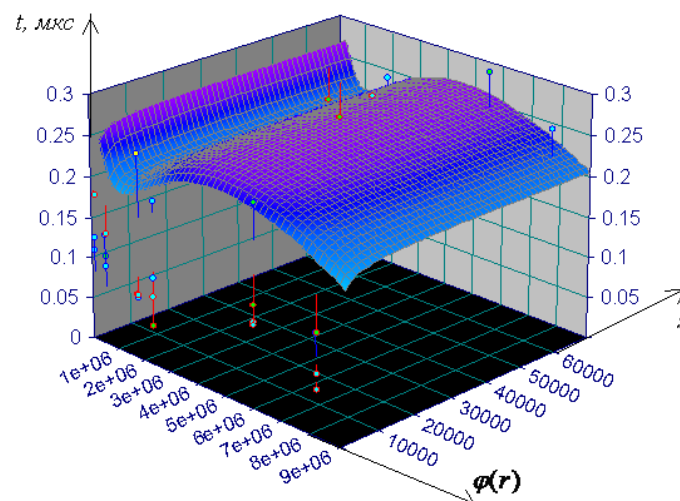


Рис. 5. Зависимость $t=F(s, \phi(r))$ для обобщённого алгоритма Евклида (Pascal)

Из приведённых зависимостей видно, что для обобщённого алгоритма Евклида время счёта колеблется в небольших пределах (0,2 мкс) и нет явных тенденций изменения (увеличение или уменьшение) с вариацией влияющих переменных.

На рисунках 6 и 7 показаны графики зависимости времени счёта от значений открытой экспоненты и функции Эйлера для алгоритмов ALGO 1 и ALGO 2.

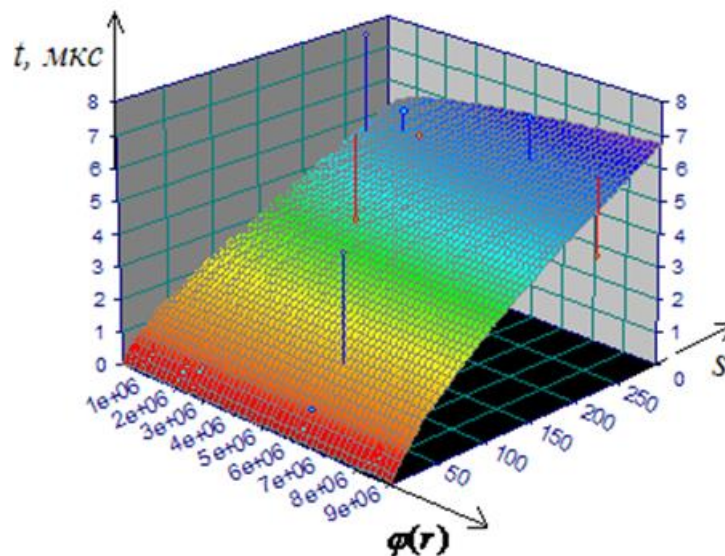


Рис. 6. Зависимость $t = F(s, \varphi(r))$ для алгоритма ALGO 1 (C#)

Из рис. 6 видна сильная зависимость времени счёта от значения открытой экспоненты. С ростом s время счёта программы, составленной по алгоритму ALGO 1, начинает в разы превышать время счёта по обобщённому алгоритму Евклида. В то же время, в области малых значений s алгоритм ALGO 1 конкурирует по быстродействию с обобщённым алгоритмом Евклида.

Анализ рис. 7 показывает, что время счёта по алгоритму ALGO 2 составляет десятки миллисекунд, что на 3...4 порядка хуже, чем у других алгоритмов. Само время счёта растёт с увеличением значений s и $\varphi(r)$.

В алгоритме ALGO 1 приближение к искомому результату идёт шагами (приращениями, квантами), равными значению функции Эйлера. Эти числа имеют большую величину, так как являются произведением двух больших чисел $p-1$ и $q-1$.

В алгоритме ALGO 2 приращения всегда равны 10, поэтому алгоритм ALGO 2 существенно проигрывает в быстродействии обобщённому алгоритму Евклида и алгоритму ALGO 1, так как для достижения большого значения секретного ключа требуется большое число итераций. В обобщённом алгоритме Евклида движение к цели происходит путём многократного поиска остатков от деления. Операция деления позволяет с большей скоростью продвигаться к цели по сравнению с увеличением величин десятками от начального числа, как это происходит в алгоритме ALGO 2.

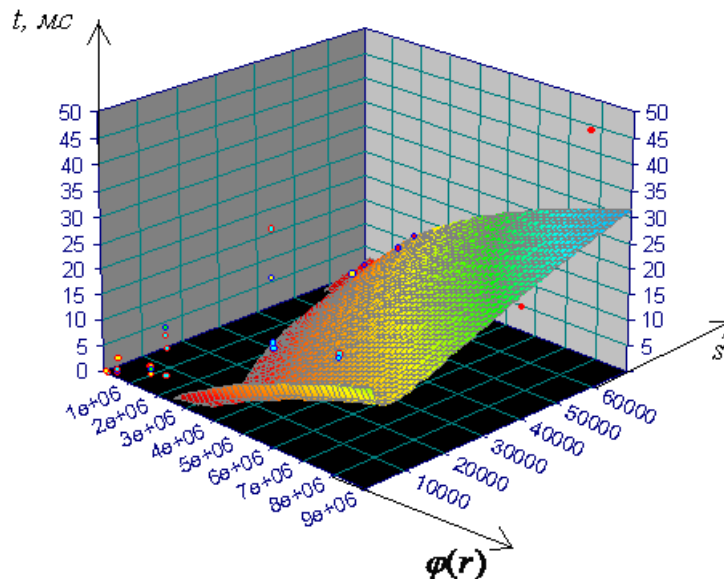


Рис. 7. Зависимость $t=F(s, \varphi(r))$ для алгоритма ALGO 2 (C#)

Для проведения сравнительного анализа алгоритмов введём величину относительного (нормированного) быстродействия R . Эта величина равна отношению времени счёта одного алгоритма ко времени счёта другого алгоритма при одинаковых значениях влияющих параметров (открытой экспоненты и функции Эйлера). Нормирование производилось ко времени счёта, затраченного на вычисления с помощью обобщённого алгоритма Евклида. Измерение времени счёта проводились в одной программной среде C# и на одном компьютере.

Величину R нужно трактовать следующим образом. Если $R=1$, то быстродействие алгоритмов одинаковое. Если $R>1$, то время счёта с помощью обобщённого алгоритма Евклида меньше, чем время счёта сопоставляемого алгоритма в R раз. При $R<1$ время счёта с помощью обобщённого алгоритма Евклида в $1/R$ раз больше по отношению к альтернативному алгоритму.

На рис. 8 показана зависимость относительного быстродействия от значений открытой экспоненты и функции Эйлера для алгоритма ALGO 1. Из графика видно, что с ростом s алгоритм ALGO 1 начинает в разы проигрывать самому быстрому алгоритму. Лишь при малых значениях открытой экспоненты $R \approx 1$ и алгоритм ALGO 1 порой опережает обобщённый алгоритм Евклида. При значениях открытой экспоненты, которые превышают значения, показанные на графике алгоритм ALGO 1, начинает проигрывать в сотни и тысячи раз.

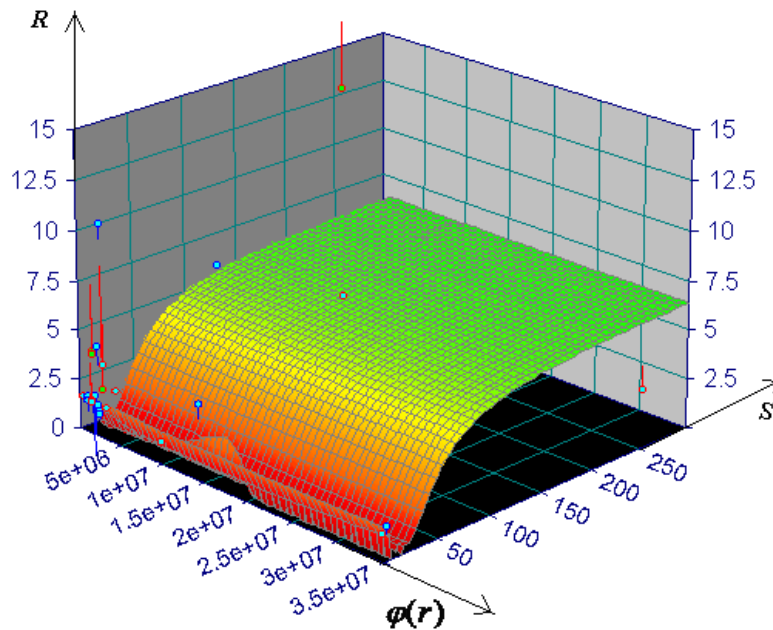


Рис. 8. Зависимость $R=F(s, \varphi(r))$ для алгоритма ALGO 1 (C#)

На следующем рисунке показана зависимость относительного быстродействия R алгоритма ALGO 2 от влияющих параметров.

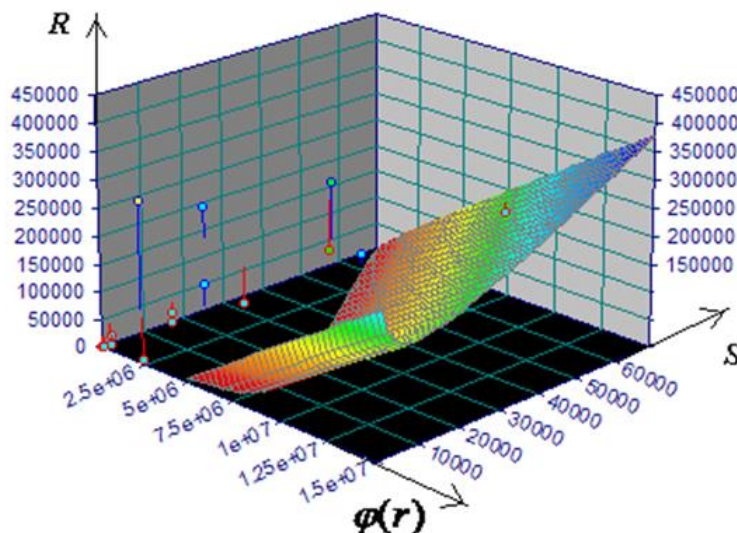


Рис. 9. Зависимость $R=F(s, \varphi(r))$ для алгоритма ALGO 2 (C#)

Время счёта по алгоритму ALGO 2 порой превышало время счёта с использованием обобщённого алгоритма Евклида в несколько сотен тысяч раз. С ростом значений открытой экспоненты и функции Эйлера алгоритм ALGO 2 всё в большей степени «отстаёт» по быстродействию от обобщённого алгоритма Эйлера. При формировании двух последних графиков расчёты проводились в одной программной среде (C#) и на одном компьютере (Lenovo ThinkCentre), поэтому результаты инвариантны по отношению к используемым при моделировании аппаратным средствам.

Выводы

Два разработанных новых алгоритма, в принципе, могут быть использованы для расчётов, так как при одинаковых исходных данных все три алгоритма дают одинаковые значения секретной экспоненты. Однако быстродействие алгоритмов различно.

Наибольшее быстродействие среди рассмотренных алгоритмов в подавляющем большинстве случаев показал обобщённый алгоритм Евклида. При малых значениях открытой экспоненты лучшие результаты порой даёт алгоритм ALGO 1. Однако, время вычисления секретной экспоненты по алгоритму ALGO 1 резко возрастает с ростом значения открытой экспоненты. Установлено, что число необходимых итераций в алгоритме ALGO 1 всегда меньше значения открытой экспоненты.

Алгоритм ALGO 2 имеет отличительные особенности только для значений функции Эйлера, кратных 10. При всех других значениях функции Эйлера расчёты ведутся с помощью обобщённого алгоритма Евклида. Время счёта по этому алгоритму на три-четыре порядка превышает время счёта по обобщённому алгоритму Евклида и ALGO 1. По этой причине этот алгоритм не может быть использован для практической реализации криптосистем.

Алгоритмы ALGO 1 и ALGO 2 удобно использовать при ручных расчётах, например, в учебном процессе при проведении практических занятий в ВУЗах для объяснения идеи шифра RSA и углублённого изучения алгоритмов формирования секретных ключей [8].

Авторы посвящают статью столетию со дня рождения Алексева Петра Андреевича.

Приложение 1.

Программа на языке Mathcad 15 для расчёта с помощью обобщённого алгоритма Евклида

Обобщенный алгоритм Евклида
Mathcad 15

ORIGIN := 1

a := 460

b := 257

$$U := \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$$

$$V := \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix}$$

$$T := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\begin{array}{l}
 k1(a,b) := \text{while } T_1 \neq 0 \\
 \quad \left| \begin{array}{l}
 U_1 \\
 c \leftarrow \frac{U_1}{V_1} \\
 q \leftarrow \text{floor}(c) \\
 T_1 \leftarrow \text{mod}(U_1, V_1) \\
 T_2 \leftarrow U_2 - q \cdot V_2 \\
 P \leftarrow T_3 \\
 P \leftarrow P + a \text{ if } P < 0 \\
 T_3 \leftarrow U_3 - q \cdot V_3 \\
 U \leftarrow V \\
 V \leftarrow T
 \end{array} \right. \\
 \quad P \\
 \\
 f(a,b) := \text{for } i \in 1..2000000 \\
 \quad \left| \begin{array}{l}
 x_i \leftarrow k1(a,b) \\
 x_i
 \end{array} \right. \\
 \\
 f(a,b) = 213
 \end{array}$$

Приложение 2.

Программа на языке Pascal для расчёта с помощью обобщённого алгоритма Евклида

```

//Обобщённый алгоритм Евклида
//PascalABC.NET Версия 2.2, сборка 1013(17.08.2015) var
U1,U2,U3,a,b,T1,T2,T3,V1,V2,V3,P,q,i:integer;
begin
Writeln('введите a и b');
readln(a,b);
U1:=a;U2:=1;U3:=0;
V1:=b;V2:=0;V3:=1;
T1:=1;T2:=1;T3:=1;
while T1>0 do
begin
q:=U1 div V1;
T1:=U1 mod V1;
T2:=U2-V2*q;
P:=T3;
If P<0 then P:=P+a;
T3:=U3-q*V3;
U1:=V1;U2:=V2;U3:=V3;
V1:=T1;V2:=T2;V3:=T3;
end;
Writeln(P);
end.

```

Приложение 3.

Программа на языке C# для расчёта с помощью обобщённого алгоритма Евклида

```
// Обобщённый алгоритм Евклида
// C#
sw.Restart();
int q = 0;
int p = 0;
for (long i = 0; i < 2000000; i++)
{
    int u1 = a, u2 = 1, u3 = 0;
    int v1 = b, v2 = 0, v3 = 1;
    int t1 = 1, t2 = 1, t3 = 1;

    while (t1 > 0)
    {
        q = u1 / v1;
        t1 = u1 % v1;
        t2 = u2 - v2 * q;
        p = t3;
        if (p < 0) p = p + a;
        t3 = u3 - q * v3;
        u1 = v1; u2 = v2; u3 = v3;
        v1 = t1; v2 = t2; v3 = t3;
    }

    sw.Stop();
    elapsed = sw.ElapsedMilliseconds;
    Console.WriteLine("Евклид = " + p);
    Console.WriteLine("Total query time: {0} ms", elapsed);
    Console.ReadKey();
}
```

Приложение 4.

Программа на языке Mathcad 15 для расчёта с помощью алгоритма ALGO 1

Алгоритм ALGO 1

Mathcad 15

$a := 460$ $b := 27$

$$k(a, b) := \left| \begin{array}{l} m \leftarrow a + 1 \\ d \leftarrow 1 \\ \text{while } d \neq 0 \\ \quad \left| \begin{array}{l} k \leftarrow \frac{m}{b} \\ d \leftarrow k - \text{floor}(k) \\ m \leftarrow m + a \end{array} \right. \\ k \end{array} \right.$$

$k(a, b) = 443$

Приложение 5.

Программа на языке Pascal для расчёта с помощью алгоритма ALGO 1

```
//Алгоритм ALGO 1
//PascalABC.NET Версия 2.2, сборка 1013(17.08.2015)
var s,f,m,y:integer;
k:real;
begin
writeln('введите s и f');//здесь s – число взаимно простое с f, так называемая
открытая экспонента; f – функция Эйлера; k-секретная экспонента
readln(s,f);

m:=f+1;
k:=m/s;
while frac(k)<>0 do//Пока остаток от деления не равен 0
begin
k:=m/s;
m:=m+f;
end;
writeln(k);
end.
```

Приложение 6.

Программа на языке C# для расчёта с помощью алгоритма ALGO 1

```
//Алгоритм ALGO 1
//C#
int a = int.Parse(Console.ReadLine());
int b = int.Parse(Console.ReadLine());

double m,k = 0;
Stopwatch sw = Stopwatch.StartNew();for (long i = 0; i < 20000; i++)
{
    m = a + 1;
    k = 0;
    while (m % b != 0)
    {
        k = m / b;
        m += a;
    }
    k = m / b;
}
sw.Stop();
long elapsed = sw.ElapsedMilliseconds;
Console.WriteLine("Алго-1= "+k);
Console.WriteLine("Total query time: {0} ms", elapsed);
Console.ReadKey();
```

Приложение 7.

Программа на языке Mathcad 15 для расчёта с помощью алгоритма ALGO 2

Алгоритм ALGO 2

Mathcad 15

a - функция Эйлера; b - открытая экспонента

a := 460

b := 27

Секретная экспонента не может быть меньше числа:

$$T_{\min} := \frac{(a+1)}{b}$$

Tmin = 17.07

Начальные значения секретной экспоненты
и переменной d:

t := 23 d := 1

```
k2(a,b) := while d ≠ 0
            n ← (b-t-1)/a
            d ← n - floor(n)
            t ← t + 10
            t - 10
```

k2(a,b) = 443

Приложение 8.

Программа на языке Pascal для расчёта с помощью алгоритма ALGO 2

//Алгоритм ALGO 2

//PascalABC.NET Версия 2.2, сборка 1013(17.08.2015)

var

f,s,i: integer;//здесь s - число взаимно простое с f, так называемая открытая экспонента; f - функция Эйлера, t-секретная экспонента

t:int64;

begin

writeln('введите s и f');//Введём функцию Эйлера f и взаимно простое с ним число s

readln(s, f);

t:=(f+1)**div** s;//Найдём t минимальное

i:=0;

if (f **mod** 10 = 0) **then** //Если f кратно 10

begin

if (s **mod** 10 = 7) **then** //Если s заканчивается на 7

begin

If (t **mod** 10<>3) **then** //Если t не заканчивается на 3

repeat t:=t+1;//Увеличиваем t на 1 пока t не будет заканчиваться на 3

until (t **mod** 10=3);

repeat t:=t+10*i;//Увеличиваем t на 10 пока не найдём нужное число для

выражения

i:=1;

until (s*t-1)**mod** f=0;

end;

if (s **mod** 10 = 3) **then**//Если s заканчивается на 3

begin

If (t **mod** 10<>7) **then**//Если t не заканчивается на 7

repeat t:=t+1;//Увеличиваем t на 1 пока t не будет заканчиваться на 7

until (t **mod** 10=7);

repeat t:=t+10*i;//Увеличиваем t на 10 пока не найдём нужное число для

выражения

i:=1;

until (s*t-1)**mod** f=0;

end;

if (s **mod** 10 = 1) **then**//Если s заканчивается на 1

begin

If (t **mod** 10<>1) **then**//Если t не заканчивается на 1

repeat t:=t+1;//Увеличиваем t на 1 пока t не будет заканчиваться на 1

until (t **mod** 10=1);

repeat t:=t+10*i;//Увеличиваем t на 10 пока не найдём нужное число для

выражения

```
        i:=1;
        until (s*t-1) mod f=0;
    end;
    if (s mod 10 = 9) then //Если s заканчивается на 9
    begin
        If (t mod 10<>9) then //Если t не заканчивается на 9
        repeat t:=t+1; //Увеличиваем t на 1 пока t не будет заканчиваться на 9
        until (t mod 10=9);
        repeat t:=t+10*i; //Увеличиваем t на 10 пока не найдём нужное число для
выражения
        i:=1;
        until (s*t-1) mod f=0;
    end;
    end
    else
        while (s<>0) and (f<>0) do
        begin
            if s > f then
                s := s mod f
            else
                f:=f mod s;
                t:=s+f;
            end;
        until (t mod 10=9);
        writeln(t); //Вывод секретной экспоненты
    end.
```

Приложение 9.

Программа на языке С# для расчёта с помощью алгоритма ALGO 2

```
// Алгоритм ALGO 2
// С#
sw.Restart();
int g = 0;
for (long i = 0; i < 2000; i++)
{
    int ss = b % 10;
    int r = 0;
    switch (ss)
    {
        case 7: r = 3; break;
        case 3: r = 7; break;
        case 1: r = 1; break;
        case 9: r = 9; break;
    }
    int t_min = (a + 1) / b;
    int t = t_min;
    for (; t % 10 != r; t++) ;
    int mm = a + 1;
    double dd = 1;
    double n;
    do
    {
        n = (b * t - 1) / (double)a;
        dd = n - Math.Floor(n);
        g = t;
        t += 10;
    } while (dd != 0);
}
sw.Stop();
elapsed = sw.ElapsedMilliseconds;
Console.WriteLine("Алго-2= " + g);
Console.WriteLine("Total query time: {0} ms", elapsed);
Console.ReadKey();
```

Приложение 10.

Расчёты на Mathcad

Алгоритм	Время, мкс	Функция Эйлера, $\varphi(r)$	Экспонента, s	Экспонента, t
Евклида	12,5	460	3	307
ALGO 1	3			
ALGO 2	26,5			
Евклида	17,8	460	17	433
ALGO 1	20			
ALGO 2	67			
Евклида	13	460	27	443
ALGO 1	31			
ALGO 2	78			
Евклида	46	460	257	213
ALGO 1	145			
ALGO 2	36,5			
Евклида	16,5	1324800	7	1135543
ALGO 1	9,5			
ALGO 2	220000			
Евклида	100	1324800	257	1211393
ALGO 1	365			
ALGO 2	260000			
Евклида	75	1324800	65537	1295873
ALGO 1	80000			
ALGO 2	235000			
Евклида	13,5	34522660	3	23015107
ALGO 1	4,1			
ALGO 2	1680000			
Евклида	27	34522660	7	24659043
ALGO 1	7,4			
ALGO 2	2800000			
Евклида	31	34522660	17	14215213
ALGO 1	10,8			
ALGO 2	1700000			
Евклида	44	34522660	257	1611953
ALGO 1	16,9			
ALGO 2	215000			

Приложение 11.

Расчёты на C#

Алгоритм	Время, мкс	Функция Эйлера, $\varphi(r)$	Экспонента, s	Экспонента, t
Евклида	0,065	460	3	307
ALGO 1	0,0635			
ALGO 2	0,6655			
Евклида	0,063	460	17	433
ALGO 1	0,4375			
ALGO 2	1,592			
Евклида	0,0625	460	27	443
ALGO 1	0,706			
ALGO 2	1,618			
Евклида	0,199	460	257	213
ALGO 1	3,213			
ALGO 2	1,093			
Евклида	0,171	1324800	7	1135543
ALGO 1	0,063			
ALGO 2	33970			
Евклида	0,176	1324800	257	1211393
ALGO 1	5,88			
ALGO 2	42160			
Евклида	0,279	1324800	65537	1295873
ALGO 1	1587,5			
ALGO 2	93335			
Евклида	0,655	34522660	3	23015107
ALGO 1	0,595			
ALGO 2	3575250			
Евклида	0,115	34522660	7	24659043
ALGO 1	0,138			
ALGO 2	6126650			
Евклида	144	34522660	17	14215213
ALGO 1	189,5			
ALGO 2	3830350			
Евклида	0,156	34522660	257	1611953
ALGO 1	0,393			
ALGO 2	450450			

Приложение 12.

Расчёты на Pascal

Алгоритм	Время, мкс	Функция Эйлера, $\varphi(r)$	Экспонента, s	Экспонента, t
Евклида	0,019	460	3	307
ALGO 1	0,0535			
ALGO 2	0,15			
Евклида	0,019	460	17	433
ALGO 1	0,34			
ALGO 2	0,44			
Евклида	0,021	460	27	443
ALGO 1	0,51			
ALGO 2	0,45			
Евклида	0,081	460	257	213
ALGO 1	2,4			
ALGO 2	0,27			
Евклида	0,019	1324800	7	1135543
ALGO 1	0,15			
ALGO 2	1150			
Евклида	0,07	1324800	257	1211393
ALGO 1	5			
ALGO 2	1500			
Евклида	0,14	1324800	65537	1295873
ALGO 1	2200			
ALGO 2	1750			
Евклида	0,02	34522660	3	23015107
ALGO 1	0,06			
ALGO 2	12222			
Евклида	0,06	34522660	7	24659043
ALGO 1	0,11			
ALGO 2	20000			
Евклида	0,08	34522660	17	14215213
ALGO 1	0,17			
ALGO 2	14000			
Евклида	0,06	34522660	257	1611953
ALGO 1	0,26			
ALGO 2	1600			

Литература

1. Молдовян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. Санкт-Петербург: БХВ-Петербург, 2005. 288 с.
2. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2010. 232 с.
3. Алексеев А. П. Информатика 2015. М.: Солон-Пресс, 2015. 400 с.
4. Фергюсон Н., Шнайер Б. Практическая криптография. М.: Издательский дом «Вильям», 2005. 424 с.
5. Sedgewick R. *Algorithms in C*. 3-е изд. Addison-Wesley Publ., 1998. 1136 p.
6. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // *Communications of the ACM*. 1978. T. 21. № 2. Pp. 120-126.
7. Алексеев А. П., Камышенков Г. Е. Использование ЭВМ для математических расчётов. Самара: Парус, 1998. 190 с.
8. Алексеев А. П. Сборник задач по дисциплине «Информатика» для ВУЗов. М.: Солон-Пресс, 2015. 104 с.

References

1. Moldovian N. A., Moldovian A. A. *Vvedenie v kriptosistemy s otkryтым kliuchom* [Introduction to Public Key Cryptosystems]. Saint-Petersburg: BHV-Petersburg Publ., 2005. 288 p. (in Russian).
2. Rjabko B. Ja., Fionov A. N. *Osnovy sovremennoj kriptografii i steganografii* [The Foundations of Modern Cryptography and Steganography]. Moscow, Gorjachaja linija-Telekom Publ., 2010. 232 p. (in Russian).
3. Alekseev A. P. *Informatika 2015* [Informatics 2015]. Moscow, SOLON-Press Publ., 2015. 400 p. (in Russian).
4. Ferguson N., Schneier B. *Practical Cryptography*. New York, John Wiley & Sons Publ., 2003. 432 p.
5. Sedgewick R. *Algorithms in C*. 3rd Ed. Addison-Wesley Publ., 1136 p. 1998.
6. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 1978, vol. 21, no. 2, pp. 120-126.
7. Alekseev A. P., Kamyshenkov G. E. *Ispol'zovanie EVM dlia matematicheskikh raschetov* [The use of Computers for Mathematical Calculations]. Samara, Parus Publ., 1998. 190 p. (in Russian).
8. Alekseev A. P. *Sbornik zadach po distsipline "Informatika" dlia VUZov*. [Problems in the discipline "Computer science" for High Schools]. Moscow, SOLON-Press Publ., 2015. 104 p. (in Russian).

Статья поступила 14 сентября 2015 г.

Информация об авторах

Алексеев Александр Петрович - кандидат технических наук, доцент, старший научный сотрудник. Профессор кафедры информатики и вычислительной техники. Поволжский государственный университет телекоммуникаций и информатики. Область научных интересов: криптография; стеганография; информатика; контрольно-измерительная техника; дефектоскопия. E-mail: apa_ivt@rambler.ru

Дикарева Ксения Николаевна – студентка. Поволжский государственный университет телекоммуникаций и информатики. Область научных интересов: криптография. E-mail: ksusha199607@yandex.ru

Макаров Максим Игоревич - кандидат технических наук. Доцент кафедры информатики и вычислительной техники. Поволжский государственный университет телекоммуникаций и информатики. Область научных интересов: криптография; стеганография; информатика. E-mail: moox700@gmail.com

Адрес: 443013, г. Самара, ул. Льва Толстого, 23.

Analysis of the Performance of Algorithms for Calculating the Secret Key in Asymmetric Cryptosystem RSA

Alekseev A. P., Dikareva K. N., Makarov M. I.

Purpose. In many publications indicates that the wrong choice of parameters RSA encryption may reduce the reliability of his. However, no mention of the fact that the public key and private key, in some cases, can completely match the subscriber and then publish the private key. The aim is to prove the possibility of forming twin keys where public and private keys are the same. **Methods.** The possibility of forming the twin keys theoretically justified with eight lemmas. **Novelty.** It is shown that for values of Euler's function, a multiple of ten, there is a possibility of publication of the private key, if the public key numbers ending in 1 or 9. **Results.** By calculation confirmed the possibility of the formation of the twin keys. **Practical relevance.** The results will improve RSA cryptographic cipher by checking for a match generated public and private keys. **Purpose.** When calculating the secret key used in the RSA cryptosystem generalized Euclidean algorithm. The article compares the performance of the generalized Euclidean algorithm with algorithms ALGO 1 and ALGO 2, developed by the authors. The aim is to conduct a comparative analysis of the performance of three algorithms for computing the secret exponent in the cryptosystem RSA. Software implementation of the algorithms implemented using three systems programming: Mathcad, Pascal and C #, allowing you to reduce the influence of the programming on the results. **Methods.** Comparative analysis of the performance of three algorithms performed by experimental method of measuring time account for different input data. Output of calculated relations for the development of algorithm ALGO 1 is made analytically. Justification algorithm ALGO 2 done by the evidence of five lemmas. **Novelty.** Developed two new algorithm for computing the secret exponents. **Results.** By calculation shows that the descending speed of the algorithms are located as follows: generalized Euclidean algorithm, ALGO 1, ALGO 2. The causes of the differences in the speed considered algorithms. **Practical relevance.** The results obtained clearly demonstrate the efficiency of solving the same problem depends on the method of solving it. The three programs discussed algorithm illustrated in programming languages Mathcad, Pascal and C #, as well as examples of manual calculations. This allows you to use the results, not only for scientific purposes, but also in the educational process

Keywords: asymmetric cryptosystem RSA, Euclidean algorithm, performance, private key, public key exponent, Euler function, Lemma, programming languages.

Information about Authors

Alekseev Aleksandr Petrovich - Ph.D. of Engineering Sciences, Associate Professor, Senior Research Officer. Professor at the Department of Computer Science and Engineering. Povolzhye State University of Telecommunications and Informatics. Field of research: cryptography; steganography, computer science; testing and measuring equipment; flaw detection. E-mail: apa_ivt@rambler.ru

Dikareva Ksenia Nikolaevna – student at the Department of Computer Science and Engineering. Povolzhye State University of Telecommunications and Informatics. Field of research: cryptography. E-mail: ksusha199607@yandex.ru.

Makarov Maxim Igorevich - Ph.D. of Engineering Sciences, Docent at the Department of Computer Science and Engineering. Povolzhye State University of Telecommunications and Informatics. Field of research: cryptography; steganography, computer science. E-mail: moox700@gmail.com

Address: Russia, 443013, Samara, L. Tolstogo Street, 23.

УДК 681.518

Тренажер для повышения эффективности обучения студентов ВУЗов и технологов литейных специальностей

Воронин Ю. Ф., Камаев В. А.

Задача работы: повышение возможности быстрого распознавания разновидностей дефектов отливок и их быстрой ликвидации. Известные способы определения разновидностей дефектов не содержат характерные отличительные особенности изучаемого брака отливок. **Целью работы** является разработка автоматизированной системы «Тренажер» предназначенной для формирования устойчивых навыков определения брака отливок, использования характерных отличительных особенностей отливок по цвету, месту расположения, величине, количеству, форме и др. Далее следует определение этапов формирования дефектов и способов их ликвидации. **Используемые методы.** Использованы визуально-логические и анимационные системы для изучения процессов возникновения дефектов в динамике заливаемого металла. **Новизна.** Элементами новизны автоматизированной системы «Тренажер» является использование визуально-логических систем определение разновидностей литейных дефектов. При изучении дефекта определяются этапы его формирования по имеющимся признакам на дефекте и отливке. Используя этапы возникновения дефектов составляются способы ликвидации возникающего брака отливок. **Результат:** использование представленного решения по ликвидации рассматриваемых дефектов отливок в виде отдельных областей приведенной выше маршрутизации, позволяет резко снизить время по изучению разновидностей дефектов отливок, а также создать новую или доработать имеющуюся технологию изготовления отливок высокого качества. **Практическая значимость.** Тренажер обеспечивает возможность быстрого распознавания разновидностей дефектов, этапов их возникновения и способов ликвидации. Это позволяет студентам получить навыки точного определения разновидности дефектов отливок, а технологам литейного производства быстро нейтрализовать условия возникновения брака литья.

Ключевые слова: отливка, качество, брак литья, системный подход, обучение, качество, тренажер, визуально-логическое определение, поэтапный анализ, ликвидация брака.

Производство качественного литья требует от литейщиков повышенных знаний о происходящих в форме физических процессах формирования отливок. Как показывает практика, у ряда специалистов встречаются затруднения в принятии правильных решений при разработке технологического проекта или выявлении и ликвидации брака отливок. В большинстве случаев происходит это от неполноты полученных знаний, как при обучении в ВУЗах, так и при получении практических навыков на производстве. Как следствие, в лучшем случае, производство бракованного литья приводит к повышению стоимости выпускаемых отливок и в худшем случае, к производственным авариям, в ряде случаев с трагическим исходом, примеры – крушения грузовых вагонов. Что же затрудняет студентам и технологам усваивать знания по бездефектному изготовлению отливок? Приведем ориентировочные результаты различных подходов к проведению лекций, которые с различной эффективностью доводят знания до слушателей.

- 1) Лекции проводятся считыванием материала из книги, рукописей или компьютера и записыванием прочитанного студентами. Внимание студентов здесь проявляется к безошибочной механической записи лекций, на что затрачивается до 25% возможностей человека.

- 2) Проведение лекций выполняется преподавателем устно с записью информации студентами, на что затрачивается до 40% возможности студентов.
- 3) Проведение преподавателем лекции устно с показом на экране информационного материала по теме занятий. При этом в библиотеке имеются учебные пособия по рассматриваемой теме. Такие лекции позволяют студентам воспринимать общую информацию до 80%.
- 4) Проведение преподавателем лекции устно с показом на экране цветного информационного материала, описывающего процессы, протекающие в литейной форме при возникновении и ликвидации рассматриваемых дефектов. При этом в библиотеке имеются цветные учебные пособия, позволяющие вспоминать материал проведенных лекций. Такие лекции позволяют студентам воспринимать до 100% информации: не менее 60% информации визуально и около 40% через слух.

Изучая производство бракованного литья на различных заводах, было установлено, что технологи литейного производства затрудняются в точном определении некоторых основных разделов процесса формирования дефектных отливок. К таким разделам можно отнести:

- определение разновидностей литейных дефектов по характерным отличительным особенностям;
- выявление этапов формирования дефектов отливок от начальной стадии заливки металла в форму до формирования дефекта в литой заготовке;
- знания о происходящих в литейной форме процессов возникновения или ликвидации литейных дефектов для последующего изменения технологического проекта.

Затруднения технологов вытекают из-за отсутствия полученных в институтах и университетах системных знаний по уверенному определению и ликвидации литейных дефектов и вытекающих отсюда знаний по разработке технологических проектов бездефектного изготовления отливок. Проверка имеющихся знаний у студентов пятого курса университетов показала значительное количество пробелов по разновидностям литейных дефектов, определению причин их возникновения и способов ликвидации. При разработке курсовых проектов по технологии изготовления отливок допускаются существенные ошибки, не замечаемые преподавателями, которые неизбежно приведут отливки к браку.

Анализируя ситуацию с подготовкой квалифицированных кадров литейщиков для машиностроительной промышленности России, следует отметить, что необходима существенная модернизация учебного курса, позволяющая студентам получать и устойчиво запоминать информацию по бездефектному изготовлению отливок. Для реализации процесса модернизации, необходимо разработать учебные пособия, позволяющие отчетливо представлять разновидности литейных дефектов и процессы, протекающие в литейной форме при заливке и затвердевании металла.

На протяжении 10 лет ученые кафедры Волгоградского государственного технического университета совместно с НПО ВНИИТМАШ и кафедрой «Литейное производство» занимались системным подходом к выявлению разновидностей литейных дефектов, причинно-следственных связей их возникновения и способов ликвидации [1-7]. Для оказания помощи технологам литейного производства и студентам ВУЗов в принятии правильных решений, на основании этих работ опубликованы 4 цветных учебных пособия [8-11] по основным группам литейных дефектов: светлым газовым раковинам, усадочным дефектам, трещинам, окисленным газовым раковинам. По материалам учебных пособий созданы 4 автоматизированные системы «Тренажер» для выработки навыков бездефектного изготовления отливок» для нейтрализации отмеченных выше четырех групп дефектов. В «тренажере» используются визуальное и логическое представления происходящих в литейной форме процессов возникновения и ликвидации литейных дефектов. Применение визуализации процессов примерно на 60% повышает усвояемость методологии повышения качества отливок студентами и технологами, поэтому тренажер является эффективным инструментом в ускоренном приобретении навыков выпуска отливок высокого качества. Каждая автоматизированная система создана для одной группы дефектов, имеющих большинство схожих отличительных признаков, описанных выше.

В Волгоградском государственном техническом университете разработаны 5 Тренажеров для повышения навыков бездефектного изготовления отливок из чугуна и стали, позволяющих улучшить визуальное восприятия получаемых знаний [3]. Информационное наполнение тренажера выполнено на основе многолетнего опыта работы в области повышения качества литья [4-8]. В Тренажер вошли практические приемы и материалы по ликвидации дефектов реальных отливок [9].

Архитектура тренажеров представлена на рис. 1. Автоматизированная система включает 3 основных блока. Главным является блок Тренажеры. С использованием Тренажеров происходит обучение пользователя идентификации и ликвидации дефекта отливок. Для повышения эффективности устранения литейных дефектов пользователю предлагается апробированная методика, позволяющая по визуальным характеристикам точно определить разновидность дефекта и способ его формирования. Кроме этого предлагаемая методика позволяет определить причину возникновения дефекта и выбрать наиболее эффективные приемы его устранения.

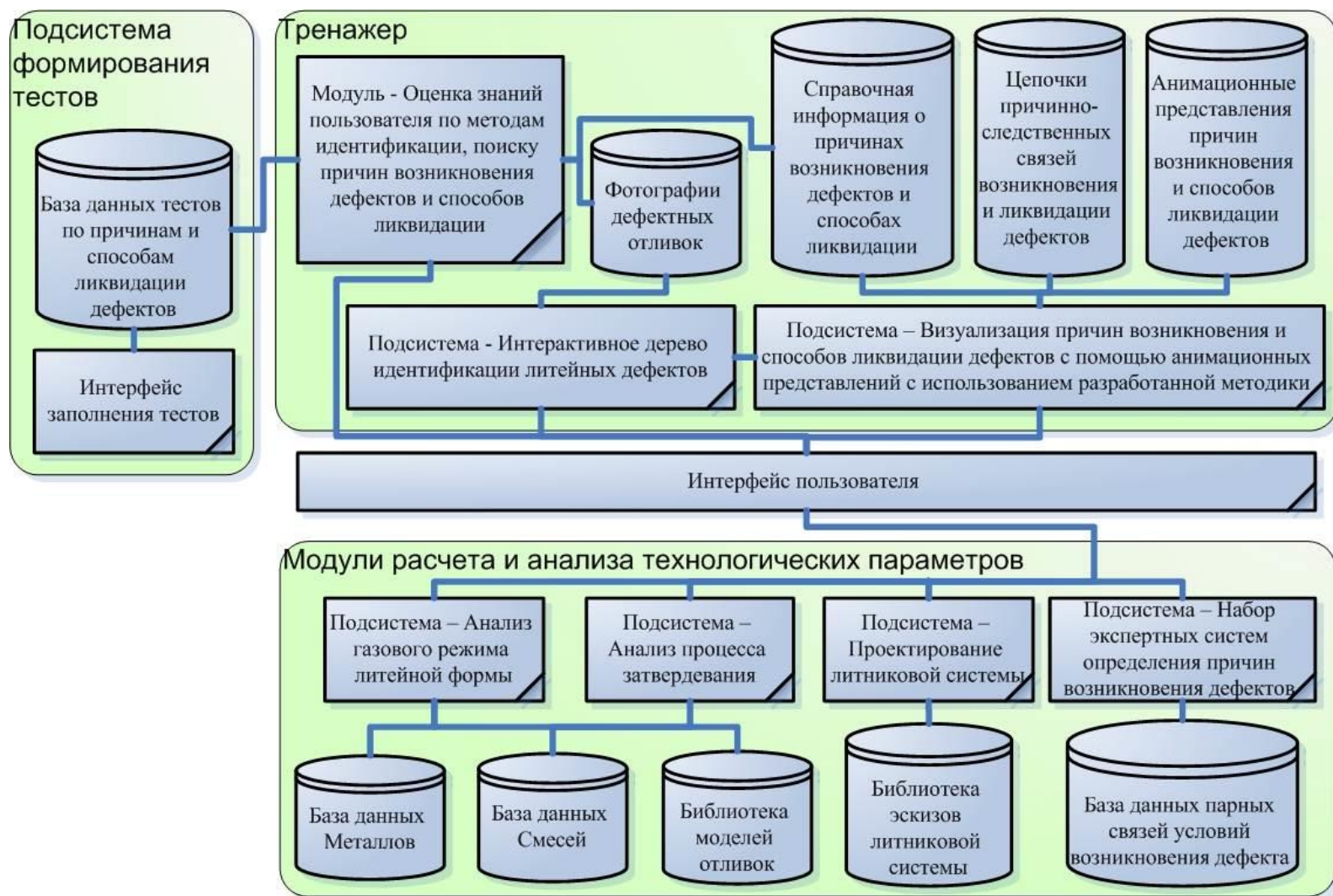


Рис. 1. Схема автоматизированного комплекса «Технологические основы устранения дефектов отливок»

Методика включает в себя:

- набор деревьев идентификации дефектов с цветными фотографиями, описанием внешнего вида поверхности и образа дефекта [10];
- цепочки причинно-следственных связей приведших к возникновению дефектов. Для каждой разновидности дефектов построены наборы цепочек, позволяющих с высокой точностью определить последовательность технологических операций приведших к возникновению дефекта;
- способы ликвидации дефектов представлены анимационными роликами, схематически демонстрирующими процессы, протекающие в литейной форме. В роликах представлены процессы, приводящие к возникновению дефектов, а также технологические приемы для повышения качества литья, с подробным описанием поэтапного устранения дефекта.

Помимо визуальных приемов, в тренажерах имеется богатейший материал по технологическим параметрам производства местами подкрепленный модулями позволяющими рассчитать основные технологические параметры и конструкционные элементы, необходимые для производства отливки.

Далее представлены фрагменты использования «Тренажера» при исследовании сложного дефекта из группы усадочных раковин - «усадочной пористости». Причина течи в изделии «Задвижка Ду300» обусловлена именно этим дефектом совместно с дефектом окисленные газовые раковины.

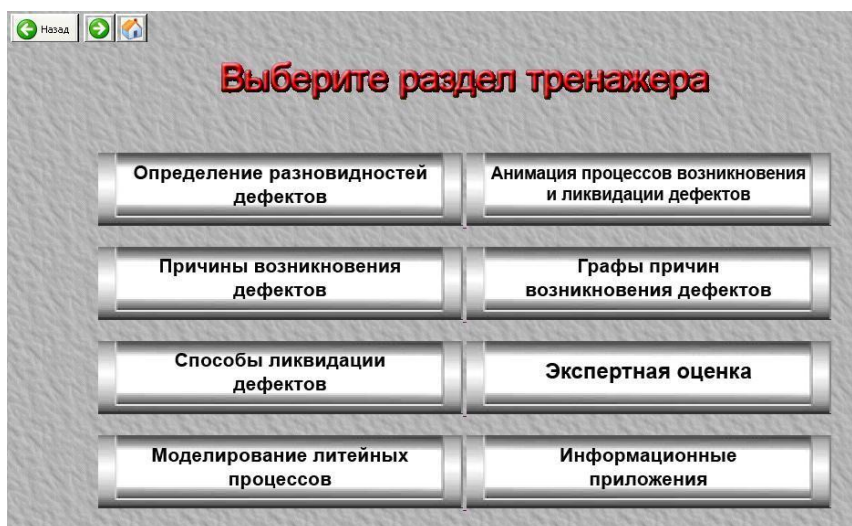


Рис. 2. Перечень рабочих разделов «Тренажера»

На рис. 2 приведены рабочие разделы «Тренажера» для проведения комплекса исследований при ликвидации дефектов отливок в следующем направлении.

- 1) Определение визуально-логическим способом разновидностей дефектов по дереву, созданному на основе системного подхода к их характерным отличиям. Контрольные вопросы по усвоению определения разновидностей дефектов усадочного происхождения.

- 2) Поэтапный анализ причин возникновения «Течи» с использованием дефектной отливки и ее сечений в направлении формирования дефекта отливки.
- 3) Анимационное (визуальное) представление полного и поэтапного процесса *возникновения* рассматриваемого дефекта. Составление цепочек причинно-следственных связей между разновидностью дефекта и причинами его возникновения.
- 4) Анимационное (визуальное) представление полного и поэтапного процесса *ликвидации* течи отливки с использованием результатов причинно-следственных связей.
- 5) Составление графов причин возникновения дефектов по составленным цепочкам причинно-следственных связей для пополнения банка данных.
- 6) Составление графов способов ликвидации дефектов полученными результатами при проведении исследований для пополнения банка данных. Контрольные вопросы по усвоению определения причин возникновения и способов ликвидации усадочных дефектов.
- 7) Информационные приложения по рассматриваемому материалу.



Рис. 3. Начальная стадия определения разновидности дефекта «Пористости»



Рис. 4. Проведение цикла определения разновидности дефекта «Пористости»

На рис. 3 показан экран начальной стадии определения разновидности дефекта по дереву дефектов. Например, дефект выбирается в группе «Несплошности в теле отливки». При активировании этой группы, на экране (рис. 4) появляются ее подразделы, где выбираются «Раковины». Нажатием мышкой на изображение фрагмента отливки, происходит его увеличение для лучшего просмотра при исследовании. Последовательным выбором представленных изображений с описаниями на экранах, спускаемся по дереву дефектов на нижний уровень и определяем разновидность исследуемого дефекта, знакомимся с механизмом его образования. Далее требуется ответить на контрольные вопросы по определению разновидностей дефектов, получить оценку и описание правильных ответов.

Следующий этап исследований состоит в определении влияния «Пористости» на возникновения брака «Течь» отливки. Отливки представлены на рис. 5, на рис. 6 приведено увеличенное место возникновения течи,

отмеченное мелом при гидроиспытании. При тщательном осмотре необработанной поверхности образования течи со стороны формы и стержня, замечены очень мелкие гладкие окисленные раковины, уходящие в сторону термического узла, в область пористости утолщенной стенки отливки (рис. 7).



Рис. 5. Исследуемые отливки с дефектом течь



Рис. 6. Увеличенное место возникновения течи отливки



Рис. 7. Механическая обработка в месте образования газовой раковины

Раковины образуются от повышенного давления газа при сгорании связующего смеси и отсутствия вентиляционной системы. При совмещении газовых раковин с пористостью в сквозную цепочку, возникает течь отливки. Процесс возникновения течи отливки «Задвижка Ду300» произошел в результате отсутствия вентиляционных наколов на поверхности формы, невыполнения вентиляционной системы в стержне и отсутствия на термических узлах отливки прибылей для подпитки усадочных мест. В результате повышения давления газа в отливке образуются узкие свищевидные раковины в направлении термического узла, в утолщенной стенке отливки формируется пористость, что создает условия для возникновения течи в отливке.

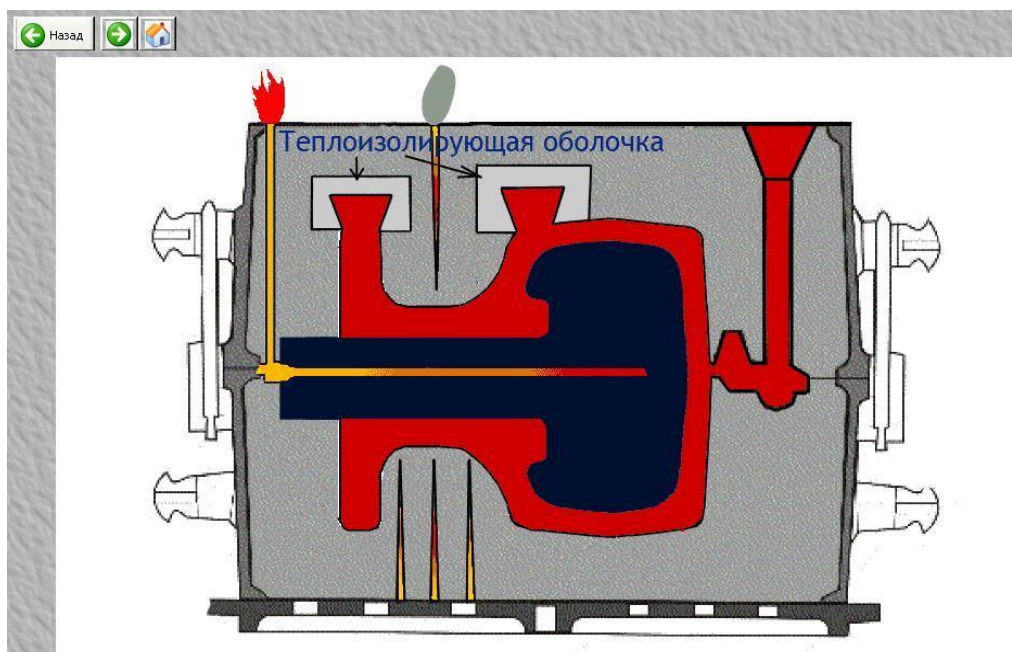


Рис. 8. Анимационный процесс ликвидации течи отливки

Далее в системе приводится и исследуется анимационный процесс ликвидации дефектов в отливке путем применения вентиляционных систем в форме и стержне, и прибылей для подпитки пористых и усадочных мест отливки (рис. 8). На рисунке видно, как происходит удаление газа из стержня и формы через вентиляционную систему (факелы) в атмосферу. Применение теплоизолирующих оболочек позволяет вдвое уменьшить объем применяемых в промышленности прибылей.

В «тренажере» приводятся графы (таблицы) причинно-следственных связей возникновения дефектов и способов их ликвидации из практики ликвидации литейных дефектов. В заключении обучения компьютер выставляет оценку по пройденному материалу. При невысокой оценке предоставляется информация для повышения знаний по рассматриваемому материалу.

Кроме описанного, в Тренажере имеются автоматизированные системы по расчету литниковых систем для чугуна и стали с выдачей через принтер рабочих чертежей, информационные материалы по рассматриваемым дефектам отливок и другое. В настоящее время тренажеры используются для обучения магистрантов в Волгоградском государственном техническом университете и проведении дистанционного повышения квалификации специалистов литейного производства на заводах.

Вывод

Использование «Тренажера» позволяет студентам и технологами литейного производства более подробно ознакомиться с эффективными подходами к процессу изготовления отливок высокого качества. Тренажер позволяет действительно увидеть процесс возникновения дефектов и их ликвидации, при использовании анимационного процесса формирования отливок. При этом Тренажер позволяет реализовать новые методики

преподавания и в конечном итоге повысить успеваемость обучающихся примерно на 25–30%.

Литература

1. Воронин Ю. Ф. Системный подход к процессу возникновения и ликвидации горячих трещин // *Литейщик России*. 2010. № 3. С. 11-14.
2. Воронин Ю. Ф., Воронин С. Ю., Лукьяненко А. Ю., Сухонослова В. Ю. Системное выявление условий возникновения и ликвидации течи отливки // *Литейщик России*. 2010. № 2. С. 10-13.
3. Воронин Ю. Ф., Лосев А. Г., Матохина А. В., Бегма В. А. Моделирование газового режима литейной формы // *Литейщик России*. 2004. № 4. С. 35-41.
4. Воронин Ю. Ф., Камаев В. А., Матохина А. В., Карпов С. А. Автоматизированная система «Атлас литейных дефектов. Чугун и сталь» // *Заготовительные производства в машиностроении*. 2004. № 6. С. 3-7.
5. Воронин Ю. Ф., Камаев В. А. Компьютер определяет причину возникновения дефекта отливки // *Литейщик России*. – 2005. № 8. С. 30–34.
6. Воронин Ю. Ф., Куликов Д. Ю. Моделирование процесса остывания отливок в литейной форме // *Программные продукты и системы*. 2007. №3. С. 61-63.
7. Воронин Ю. Ф., Куликов Д. Ю. Моделирование условий снижения или ликвидации усадочных дефектов // *Оборудование. Технический альманах*. 2006. № 3. С. 34-39.
8. Воронин Ю. Ф. Система определения и ликвидации трещин в отливках из чугуна и стали. Учебное пособие. – Волгоград: Волгоградский государственный технический университет, 2010. – 149 с.
9. Воронин Ю. Ф. Система определения и ликвидации усадочных дефектов в отливках из чугуна и стали. Учебное пособие. – Волгоград, Волгоградский государственный технический университет, 2010. – 139 с.
10. Воронин Ю. Ф. Система определения и ликвидации светлых газовых раковин в отливках из чугуна и стали. Учебное пособие. – Волгоград: Волгоградский государственный технический университет, 2010. – 124 с.
11. Воронин Ю. Ф. Система определения и ликвидации окисленных газовых раковин в отливках из чугуна и стали Учебное пособие. – Волгоград: Волгоградский государственный технический университет, 2010. – 116 с.

References

1. Voronin Iu. F. A systematic approach to the process of emergence and elimination of hot cracks. *Liteishchik Rossii*, 2010, no. 3, pp. 11-14 (in Russian).
2. Voronin Iu. F., Voronin S. Iu., Luk'ianenko A. Iu., Sukhonosova V. Iu. A system to identify the conditions of emergence and elimination of leaks casting. *Liteishchik Rossii*, 2010, no. 2, pp. 10-13 (in Russian).
3. Voronin Iu. F., Losev A. G., Matokhina A. V., Begma V. A. Modeling of gas mode mold. *Liteishchik Rossii*, 2004, no. 4, pp. 35-41 (in Russian).

4. Voronin Iu. F., Kamaev V. A., Matokhina A. V., Karpov S. A. Automated system "Atlas of casting defects. Iron and steel". *Zagotovitel'nye proizvodstva v mashinostroenii*, 2004, no. 6. pp. 3-7 (in Russian).
5. Voronin Iu. F., Kamaev V. A. The computer determines the cause of occurrence of defect of casting. *Liteishchik Rossii*, 2005, no. 8, pp. 30-34 (in Russian).
6. Voronin Iu. F., Kulikov D. Iu. Modelling of process of cooling of castings in the mold. *Programmnye produkty i sistemy*, 2007, no. 3, pp. 61-63 (in Russian).
7. Voronin Iu. F., Kulikov D. Iu. The modeling of the reduction or elimination of shrinkage defects. *Oborudovanie. Tekhnicheskii al'manakh*, 2006, no. 3, pp. 34-39 (in Russian).
8. Voronin Iu. F. *Sistema opredeleniia i likvidatsii treshchin v otlivkakh iz chuguna i stali* [System definition and elimination of cracks in the castings of iron and steel]. Volgograd, Volgograd State University, 2010, 149 p. (in Russian).
9. Voronin Iu. F. *Sistema opredeleniia i likvidatsii usadochnykh defektov v otlivkakh iz chuguna i stali*. [System definition and elimination of shrinkage defects in the castings of iron and steel]. Volgograd, Volgograd State University, 2010, 139 p. (in Russian).
10. Voronin Iu. F. *Sistema opredeleniia i likvidatsii svetlykh gazovykh rakovin v otlivkakh iz chuguna i stali* [System definition and elimination of light gas pockets in the castings of iron and steel]. Volgograd, Volgograd State University, 2010, 124 p. (in Russian).
11. Voronin Iu. F. *Sistema opredeleniia i likvidatsii okislennykh gazovykh rakovin v otlivkakh iz chuguna i stali* [System definition and elimination of the oxidized gas pockets in the castings of iron and steel]. Volgograd, Volgograd State University, 2010, 116 p. (in Russian).

Статья поступила 5 октября 2015 г.

Информация об авторах

Воронин Юрий Федорович – доктор технических наук. Профессор кафедры «Системы автоматизированного проектирования и программного конструирования». Волгоградский государственный технический университет. Область научных интересов: системы автоматизированного проектирования; сбор и обработка информации для создания автоматизированных систем повышения качества отливок из чугуна и стали. E-mail: voronin@vstu.ru

Камаев Валерий Анатольевич – доктор технических наук, профессор. Заведующий кафедрой «Системы автоматизированного проектирования и программного конструирования». Волгоградский государственный технический университет. Область научных интересов: концептуальное проектирование изделий и технологий; системы автоматизированного проектирования. E-mail: vkamaev40@mail.ru

Адрес: Россия, 400131, г. Волгоград, пр. Ленина, д. 28.

Training Apparatus, as Means of Increase of a Learning Efficiency of Students of High Schools and Technologists of Foundry Specialties

J. F. Voronin, V. A. Kamayev

Statement of the problem. Students casting professions should be able to quickly identify and eliminate the defects of castings. However, training tools do not contain visualization of the distinctive features of defects and their causes. **The purpose of work** is to develop automated training tools "simulator" which is designed to teach the definition of defects castings. "Simulator" is based on the visualization of the stages of formation and the causes of defects. **The methods used.** The logical schemata and animated videos use for visualize the stages of formation of defects. **Novelty.** The training tool "simulator" uses the new visual logical system for finding defects and determines they types. "Simulator" allows to reasonably choosing the method of elimination of arising defects. **Practical relevance.** Students who use "simulator", can determine the type of defect, stage of the formation of defects and to choose a method of removal of defects. This is the training tool being used to teach students of casting professions can improve student performance by about 25-30%.

Key words: casting, quality, moulding marriage, the system approach, training, quality, a training apparatus, visually-logic definition, the stage-by-stage analysis, marriage liquidation.

Information about Authors

Jury Fedorovich Voronin - Dr. habil of Engineering Sciences. Professor at the Department of System Automatic Engineering and Program construction. Volgograd state technical university. Field of research: CAD system; accumulation and processing of information to create automated systems to improve the quality of castings from cast iron and steel. E-mail: voronin@vstu.ru

Valery Anatolevich Kamayev - Dr. habil of Engineering Sciences, Full Professor. Head of the Department of of System Automatic Engineering and Program construction. Volgograd state technical university. Field of research: conceptual design of products and technologies; CAD systems. E-mail: vkamaev40@mail.ru

Address: Russia, 400131, Volgograd, Lenina prospekt, 28.