SCCS

Системы управления, связи и безопасности

Systems of Control, Communication and Security

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

№3 2016

ISSN 2410-9916

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 2016 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

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

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.

Требования к оформлению статей, представляемых в редакцию

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 – A4. 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 станицах, 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 соотсветсвии 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 треюования:

- 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 – 12,6 Мб.
Комплектация издания – 1 CD.
Тираж 100 экз.

УДК 621.39

Экспертно-квалиметрический метод интегральной оценки эффективности инновационных проектов и применения новых технологий

Кузовкова Т. А., Кузовков Д. В., Кузовков А. Д.

Постановка задачи: *высокие темпы научно-технического прогресса и значение инновационного развития инфокоммуникаций, разнообразие положительных и отрицательных сторон социально-экономической эффективности инноваций актуализируют разработку новых качественных методов интегральной оценки эффективности инновационных проектов.* ***Целью работы*** *является, во-первых, обоснование экспертно-квалиметрического метода оценки эффективности и выбора наиболее эффективных инноваций из множества альтернатив; во-вторых, применение данного метода для интегральной оценки эффективности инновационных решений и внедрения новых технологий.* ***Используемые методы:*** *экспертно-квалиметрический метод основан на методах квалиметрии, экспертного оценивания, построения комплексных показателей и статистических методах анализа вариации и характера распределения.* ***Новизна:*** *новизной обладает предложенный экспертно-квалиметрический метод оценки эффективности и выбора наиболее эффективных инноваций из множества альтернатив на основе количественного измерения экспертами параметров модели, расчета коэффициента эффективности и ранжирования инноваций.* ***Результат:*** *формирование методического аппарата интегральной оценки эффективности инновационных решений и внедрения новых технологий позволяет повысить степень обоснованности решений инновационного менеджмента вследствие количественной оценки экспертами множества качественных параметров социально-экономической эффективности.* ***Практическая значимость:*** *представленное решение предлагается использовать в системе оценки эффективности инновационных проектов. Реализация экспертно-квалиметрического метода интегральной оценки эффективности инновационных проектов дает возможность более объективно обосновывать решения по выбору наиболее эффективных инноваций, вариантов построения систем и оценивать эффективность внедрения новых технологий, в том числе инфокоммуникационных технологий, с учетом воздействия множества факторов.*

Ключевые слова: *эффективность, инновации, инновационные решения, квалиметрия, экспертные оценки, интегральный коэффициент эффективности, инфокоммуникации.*

Введение

Высокие темпы научно-технического прогресса в области инфокоммуникаций, структурная трансформация отраслевой экономики и рыночной конъюнктуры, насыщение рынка традиционными услугами определяют большую роль инновационного развития. Для обеспечения устойчивого развития и конкурентоспособности компании связи должны своевременно распознавать инновации, ведущие к технологическому прорыву и созданию конкурентных преимуществ, и направлять инвестиции в высоко эффективные технологии, стандарты, сети и услуги.

Решение задачи обоснования выбора эффективных направлений развития, построения сетей и систем, инноваций в сфере инфокоммуникаций связано с рядом таких трудностей как: отсутствие количественно выраженной информации по результатам, ресурсам и потребностям их реализации на рынке на перспективный период, особенно на ранних стадиях жизненного цикла инноваций; быстрота и масштабы появления инноваций, отражающих одни и те

же потребности; различный спрос по территориям потребления; жесткая конкуренция на мировых рынках услуг связи.

Известные методы инновационного менеджмента не могут в полной мере решить задачу многокритериального отбора из множества альтернатив наиболее эффективных инноваций и направлений функционирования систем. Решение такой сложной задачи возможно на основе комплексного подхода и применения квалиметрических методов и моделей построения интегральных показателей в сочетании с экспертным способом измерения различных параметров эффективности.

Для обоснования выбора наиболее эффективных инноваций по разным видам связи, группам потребителей и территориям оказания услуг предлагается использовать экспертно-квалиметрический метод (ЭКМ) измерения эффективности инноваций по комплексной системе показателей, количественно оцениваемых с помощью экспертного метода. Данный подход был впервые предложен немецкими специалистами и усовершенствован российскими учеными.

В основе экспертно-квалиметрического подхода лежат методы экспертной оценки индикаторов эффекта и затрат в баллах и научные принципы квалиметрии в области построения комплексных показателей оценки эффективности инноваций как совокупности отдельных свойств, количественно измеряемых с помощью интервальных шкал. Формированию надежного и достоверного аппарата обоснования выбора наиболее эффективных направлений развития систем, технологий и инноваций служит также методология построения интегральных моделей эффективности, процедура экспертной оценки и комплексного измерения параметров эффективности.

Предложенный комплексный подход к обоснованию стратегии инновационного развития на основе интегрального и экспертно-квалиметрического методов имеет научно-практическое значение для всех участников рынка в сфере инфокоммуникаций, операторов связи и производителей оборудования, регулирующих органов, заинтересованных в принятии эффективных управленческих решений по инновационному развитию, внедрению новых и усовершенствованных технологий, стандартов, сетей и услуг.

Задачи инновационного менеджмента и методы оценки эффективности инновационных решений

Современные условия развития и функционирования инфокоммуникаций самым тесным и непосредственным образом связаны с постоянно возрастающим воздействием на хозяйствующие субъекты широкого спектра внешних и внутренних факторов, в том числе дестабилизирующих и деструктивных факторов как неотъемлемых элементов рыночной экономики.

Опережающие темпы развития науки, техники и технологий в сфере инфокоммуникаций и сопряженных секторов экономики, жесткая конкуренция на рынках инфокоммуникационных услуг, резкие колебания фондовых и валютных курсов, неконтролируемая инфляция, нестабильные уровни спроса и

предложения, сопровождающиеся переходом пользователей от фиксированных видов связи к беспроводным, гипердинамично изменяющаяся законодательная база, а также многие другие внешнеполитические и внутренние факторы создают затруднительные условия реализации любых стратегических планов и прогнозов с заведомо гарантированным успехом [1, 2].

Выжить в условиях интенсивной конкурентной борьбы хозяйствующим субъектам – организациям связи позволяет, в первую очередь, использование научно обоснованных методов и механизмов управленческой деятельности, в основе которых лежит процесс системного решения постановки и достижения стратегических целей развития организаций [3, 4, 5]. Не смотря на обилие публикаций и предложений по стратегическому управлению практически ни одна организация не может продемонстрировать удачный пример эффективного стратегического менеджмента.

Одной из важнейших проблем стратегического управления до сегодняшнего дня остается степень обоснованности выбора того или иного направления развития. Даже при ограниченном числе целей всегда есть альтернатива. При этом подавляющее число известных решений стратегического менеджмента сводится к применению известных стоимостных методик оценки эффективности проектов, построению матриц и диаграмм, которые не дают полноты картины не в отношении реальных доходов и затрат по отдельным направлениям, ни по числу учитываемых факторов.

При этом преобладает распространение принципов долгосрочного планирования на основе переноса экстраполяции сложившихся тенденций, динамики финансово-экономических показателей на будущее. Тогда как процесс стратегического планирования предполагает, что на каждом отрезке времени должны выбираться альтернативы, позволяющие достичь целей наиболее эффективными способами и с наибольшим эффектом [4, 6, 7, 8, 9]. Кроме того, при разработке необходимо учитывать различные риски, особенно в части изменения тарифов на элементы производственных ресурсов (электроэнергии, связи, транспортных перевозок). По мнению А.Н. Фомичева «Основной целью стратегического менеджмента является обеспечение организации долгосрочного и устойчивого преимущества над оппонентами в рыночной конкурентной борьбе» [5, с. 11]. И здесь огромная роль принадлежит методам выбора наиболее оптимального варианта инновационной стратегии развития [5, с. 116].

В период жесткой рыночной конкуренции и ускоренного научно-технического прогресса в целях сохранения лидирующих позиций на рынке операторам связи приходиться постоянно пересматривать свою инновационную политику [8, 10, 11]. Под инновационной политикой следует понимать совокупность управленческих методов, обеспечивающих интеграцию всех видов нововведений и создание условий для реализации инновации во всех областях производственно-рыночной деятельности. Применение адекватных методов инновационного менеджмента обеспечивают единство науки, техники, производства и потребления, называемого инновационным пространством [11, с. 18].

Инновационная политика оператора связи является частью инновационного пространства, представляющего собой систему взаимосвязей и взаимозависимостей между научно-техническим прогрессом (НТП)_, новыми технологиями, новыми услугами, оператором связи и рыночной средой (рис. 1). Представленная схема взаимосвязей показывает, что процесс преобразования результатов НТП (изобретений, открытий) в новые технологии и услуги осуществляется путем коммерциализации в рыночной среде и принятия инновации потребителем. Отсюда вытекает значение инновационной политики оператора связи в продвижении новых технологий и услуг на рынок, развитии рынка инноваций и собственном развитии организации.

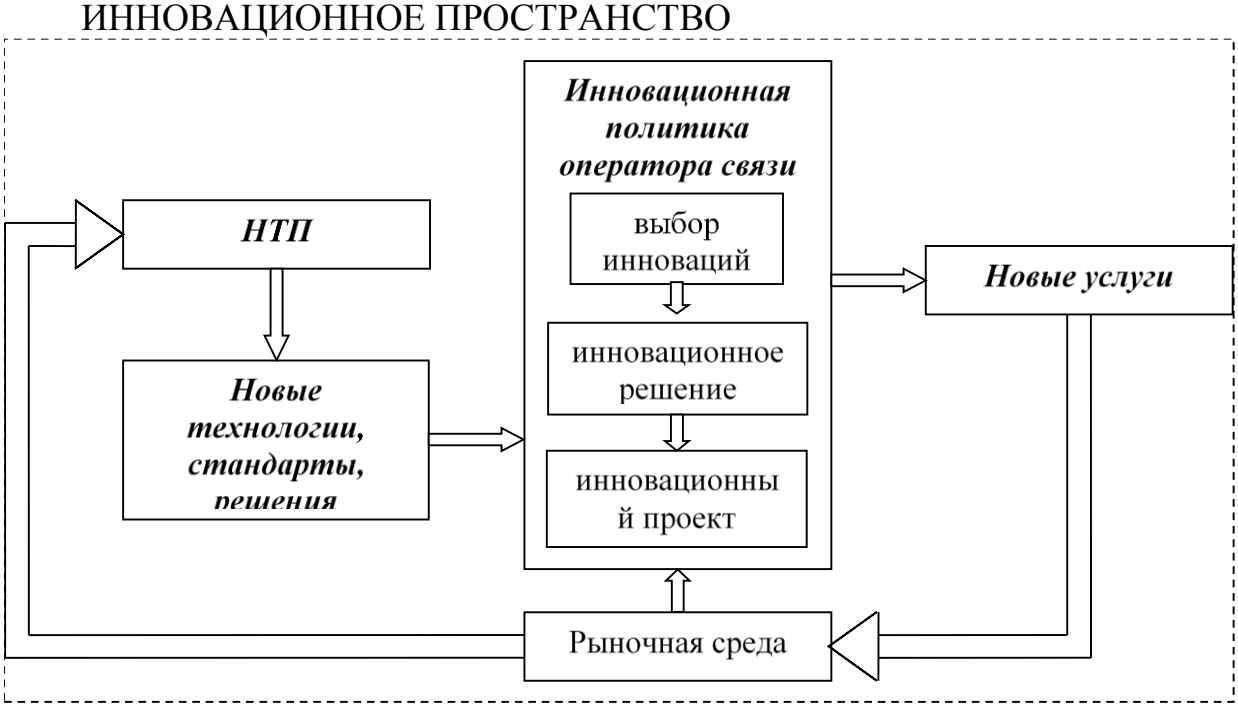


Рис. 1. Взаимосвязь инновационной политики оператора связи с элементами инновационного пространства

В современной научной литературе по инновационному менеджменту методы оценки эффективности инноваций сводятся к методологии измерения эффективности инвестиционных и инновационных проектов на основе стоимостных показателей [12-18]. При принятии решений о вводе инноваций предприятие разрабатывает инновационный проект, оценивает его эффективность по принятой методике [16]. После этого начинается следующий этап – внедрение на рынок инноваций.

Большинство инновационных проектов в инфокоммуникациях носят инвестиционный характер, то есть для осуществления проекта необходимо определить величину инвестиций, в качестве которых могут выступать как материальные, так и нематериальные средства, то есть финансовые средства, акции, ценные бумаги, техника, а также технология, лицензии, НИОКР и другие интеллектуальные ценности. В целом при оценке эффективности инновационного проекта применяют два подхода по выбранному

соотношению: превышение конечных результатов от использования инноваций над затратами на их приобретение и установку, и сопоставление полученных результатов с результатами от применения других аналогичных по назначению типов инноваций [19].

Оценка эффективности использования инвестируемого капитала производится путем сопоставления во времени отдач от инвестирования с суммой инвестиций, называемой анализом денежного потока (cash flow), который формируется в процессе реализации инвестиционного проекта. Проект признается эффективным, если обеспечивается возврат исходной суммы инвестиций и требуемая доходность для инвесторов. Инвестируемый капитал, равно как и денежный поток, приводится к настоящему времени или к расчетному году (который, как правило, предшествует началу реализации проекта). Процесс дисконтирования капитальных вложений и денежных потоков производится по различным ставкам дисконта, которые определяются в зависимости от особенностей инвестиционных проектов.

Для оценки эффективности инвестиционных проектов используют несколько показателей, которые составляют основу финансовой модели и являются базой для принятия решения о целесообразности внедрения услуги: прибыль и рентабельность инвестиций (ROI), точка безубыточности, период окупаемости (PP), чистая текущая стоимость или чистый дисконтированный доход (NPV), внутренняя норма рентабельности (IRR), индекс доходности проекта (PI), дисконтированный период окупаемости (ДРР).

Совокупность этих показателей имеет определенные достоинства, однако не учитывает результаты проекта за пределами установленного периода, влияние различных факторов рыночной среды и рисков внедрения инноваций. Укрупненные расчеты эффективности инновационного проекта на стадиях фундаментальных и поисковых исследований, прикладных исследований и разработок, т.е. на начальных стадиях жизненного цикла инноваций, далеки от реальности, что ведет к отступлению ожидаемых результатов от фактических и недостоверности оценочных показателей.

Известные методы оценки эффективности инвестиционных проектов, основанные на стоимостных показателях затрат (инвестиций) и результатов (доходов) от реализации проекта, не удовлетворяют задачам оценки эффективности инновационного развития инфокоммуникаций в условиях множества воздействующих факторов с учетом совокупности государственных, коммерческих и потребительских интересов, решения задач создания информационного общества на основе обеспечения повсеместной и недискриминационной доступности инфокоммуникационной инфраструктуры.

Необходимость совершенствования методов оценки эффективности инновационных решений в сфере инфокоммуникаций

Высокие темпы научно-технического прогресса в сфере связи и сопряженных отраслях экономики в условиях рыночных принципов хозяйствования, обострения конкуренции и повышения роли потребителя определяют необходимость совершенствования методов оценки эффективности

инновационных решений на основе учета множества параметров процесса создания, производства и реализации новых продуктов, услуг, технологий. Поскольку выведение на рынок и реализация инновационных продуктов связаны не только с техническими и экономическими проблемами их создания, масштабами реализации, но и с рисками восприятия пользователями, то для оценки эффективности инновационных проектов традиционных методов стоимостного измерения эффекта становится явно недостаточно, а порой они «не работают», оставаясь условными расчетными величинами.

Эффекты инновационного развития в сфере инфокоммуникаций затрагивают все рыночное пространство, включая производителей услуг, оборудования, потребителей услуг, контент- и сервис-провайдеров, на котором происходят существенные сдвиги в объемах и составе производственных ресурсов, спроса и предложения услуг инфокоммуникаций и смежных рынков, а также рост качества трудовых ресурсов и жизнедеятельности пользователей. При этом период реализации инвестиционного проекта занимает меньший промежуток времени, чем создание, внедрение и эксплуатация инноваций. Достижение конечного результата инновационного процесса связано с более высокими рисками по сравнению с инвестиционным проектом, в том числе с рисками готовности рынка к потреблению инновационных продуктов и услуг.

Методика оценки эффективности инноваций должна базироваться на системе показателей, учитывающих интересы всех участников инновационного процесса, в то время как методы оценки эффективности инвестиций дублируют друг друга и позволяют оценить эффективность инвестиционного проекта лишь с позиций инвестора при заданных им ограничениях. Методы оценки эффективности инноваций должны включать показатели, отражающие интегральный (внешний и внутренний) эффект от создания, производства и эксплуатации нововведений.

Такой подход позволяет не только дать обобщающую (комплексную) оценку эффективности инновационного объекта (направления развития, построения системы, инновации), но и определить вклад каждого из участников инвестиционной деятельности в эту эффективность. В отличие от этого стандартные методы оценки эффективности инвестиций позволяют определить эффективность лишь у того участника, который реализует инвестиционный проект.

Понятия эффект (effect), эффективность (effectiveness, efficiency) относятся к общим экономическим категориям, имеющим множество определений [8, 14, 20]. Экономический эффект показывает конечный результат деятельности, измеряемый стоимостными величинами, обычно разностью между доходами от деятельности и расходами на ее осуществление [15]. Под экономической эффективностью понимают результативность экономической деятельности (проектов) как отношение полученного экономического эффекта к затратам факторов производства, обусловившим получение этого результата.

В то же время термин «эффективный» означает «приводящий к каким-то результатам», «способный приносить результат», «производящий хороший

результат» [19, 20], т.е. экономический эффект характеризуется множественностью проявлений результатов, итогов деятельности. Повышение эффекта или эффективности системы в результате каких-то действий технического, организационного и экономического характера выражается целой совокупностью показателей улучшения качества товаров, услуг, работы; технического, организационного, интеллектуального уровня производства; изменения концентрации и структуры рыночной среды, конкуренции; роста конкурентоспособности и т.д., не имеющих стоимостных измерителей. При высокой значимости экономической и финансовой составляющих эффективности инновационных проектов не менее ценными являются научно-технический, производственно-ресурсный и социальный эффекты (рис. 2).

Рис. 2. Основные компоненты эффективности инновационного развития инфокоммуникаций

Эффективность инновационных проектов, обеспечивающих качественное обновление факторов производства, смену поколений техники и технологий, появление новых и усовершенствованных продуктов и услуг, совершенствование производственных процессов, характеризуется множеством проявлений и последствий не только во внутренней, но и внешней среде предприятия, что предопределяет комплексный характер оценок эффективности.

Для получения комплексной оценки эффективности инноваций или вариантов построения систем связи необходима разработка организационно-методического инструментария обоснования выбора наиболее эффективного варианта с учетом комплекса факторов и синергетического эффекта [11, 21]. При этом следует учесть, что большинство сравниваемых показателей

вариантов внедрения новых технологий или построения систем не имеют количественного выражения или отсутствуют в виде статистических или выборочных данных. Действующая же система показателей оценки эффективности инновационных проектов включает, главным образом, стоимостные методы измерения динамических и статических показателей. Действующая и предлагаемая система показателей оценки эффективности инновационных проектов представлена на рис. 3.

Рис. 3. Действующая и предлагаемая система показателей оценки эффективности инноваций

Система показателей эффективности инновационных решений должна не только определять интегральный уровень возможного состояния, динамики и потенциала развития любого объекта оценки эффективности, но и возможность ранжирования и выбора наиболее эффективных объектов.

Принятие научно обоснованных управленческих решений по повышению эффективности инновационных объектов зависит от используемого аналитического инструментария и теоретического арсенала знаний, находящихся в распоряжении современной теории и практики экономического анализа [22 - 24]. Для получения количественных или качественных оценок в целях выбора эффективных направлений развития, вариантов построения системы, инноваций могут быть использованы экспертные технологии, методы квалиметрии и комплексного оценивания [25-31].

Комплексная оценка является важным инструментом экономического анализа, индикатором состояния, критерием сравнительного оценивания деятельности хозяйствующих субъектов, основой выбора вариантов развития и принятия управленческих решений. Для того чтобы комплексная оценка была действенным инструментом инновационного менеджмента и выбора эффективных инновационных вариантов, необходимо обоснование методов ее конструирования и измерения на основе сведения различных показателей (по сущности, единицам измерения и охвата территории, методам расчета) в единый интегральный показатель.

Для комплексной оценки результатов деятельности А.Д. Шеремет [24, с. 266-267] рекомендует применять среднюю арифметическую взвешенную (суммирование показателей с учетом веса каждого показателя по какому-либо принципу) и следующие экономико-математические методы: сумм, когда суммируются фактические показатели или их отношения; суммы мест, когда суммируются места, достигнутые субъектом анализа; методы балльной оценки, когда каждый показатель имеет свой весовой балл, и «расстояний» для рейтинговой оценки субъектов анализа.

Использование различных методов исчисления интегрального показателя эффективности дает возможность получить интегральную оценку эффективности вариантов построения систем и сетей связи на основе интегрирования оценок различных сторон деятельности: рыночной, технической, социально-экономической и других. Для обоснования целесообразности включения отдельных частных показателей в систему обобщающих и, соответственно, в интегральный показатель эффективности инновационных решений в наибольшей степени подходят известные методы сумм, средней геометрической и расстояний.

Достоинства методологии интегральной оценки эффективности управленческих решений состоят в следующем:

- отражает комплексный, многомерный подход к оценке построения сложной, динамичной, открытой системы инфокоммуникаций, функционирующей в рыночной среде;
- осуществляется в условиях отсутствия статистической открытой отчетности на основе данных единовременного экспертного обследования;
- является сравнительной характеристикой, показывающей узкие места и факторы достижения более высокого уровня эффективности;
- четкий алгоритм вычислений позволяет реализовать математическую модель в компьютерном режиме.

Аналитический инструментарий комплексной оценки эффективности дополняет квалиметрия – научная область, объединяющая методы количественной оценки качества и конкурентоспособности различных объектов [25, 29-31]. На наш взгляд, необходимость применения квалиметрии к проблеме обоснования выбора наиболее эффективных инноваций из совокупности отобранных экспертами инноваций определяется множественностью эффектов их внедрения, ряд которых не может быть выражен в абсолютных или

относительных категориях стоимости, неопределенностью последствий выхода инноваций на рынок, а также технической сложностью внедрения оборудования и сетей в сфере инфокоммуникаций, которые должны быть сопряжены и совместимы по техническим параметрам [19].

На основе изучения квалиметрии как «научной области, объединяющей методы количественной оценки качества различных объектов» [30, с. 8], были отобраны методы измерения показателей качества, способы и процедуры его оценивания, а также методы комплексной оценки уровня качества. Поскольку «оценочные показатели, характеризующие свойства продукции, связанные с ее способностью удовлетворять определенные потребности» [30, с. 50] сложно измерить, то их разделяют на показатели, определяющие функциональную пригодность (назначение, надежность, технологические возможность и т.д.) и показатели, определяющие эффекты использования ресурсов на создание продукта или услуги (себестоимость, рентабельность и др.).

Данный принцип необходимо использовать для проведения процедуры выбора инноваций в сфере инфокоммуникаций в два этапа. На первом этапе из множества альтернатив должны выбираться наиболее актуальные с точки зрения технологичности, прогрессивности использования, совместимости с существующими стандартами и востребованности на рынке услуг и технических решений. На втором этапе из множества актуальных инноваций выбираются наиболее эффективные по экономическим соображениям результативности, рыночного потенциала и потребительского спроса, экономии ресурсов, снижения себестоимости, рисков реализации и запусков спутников на околоземную орбиту.

Для решения поставленных задач наибольшее значение имеют методы измерения показателей качества, способы и процедуры его оценивания, а также методы комплексной оценки уровня качества. В отличие от дифференциального метода оценки и метода главного показателя, которые позволяют фиксировать качество по отдельным показателям, метод комплексной оценки по средневзвешенному показателю позволяет производить оценку качества по совокупности показателей:

$$Q = \sum_{i=1}^{n} m_i \cdot q_i \,, \qquad (1)$$

где q_i - i–тый показатель качества;

m_i - вес i–го показателя качества (отн. ед.);

n - количество показателей качества.

Применение интегрального показателя качества I как технико-экономического показателя качества, основанного на сопоставлении суммарного полезного эффекта Э от эксплуатации или потребления продукции и суммарных затрат З на их создание и эксплуатацию: I=Э/З, ограничено теми случаями, когда эффект и затраты могут быть выражены в натуральной или денежной форме [30, с. 66]. На наш взгляд, включение в числитель и знаменатель этой формулы средневзвешенных показателей, отображающих разные аспекты качества, существенно расширяет область применения интегрального метода, в том числе и для оценки эффективности инноваций.

Применение обобщенного дифференциального метода дает двухмерную интерпретацию оценки уровня качества, причем оценка осуществляется по двум показателям, имеющим одинаковую направленность измерителей (например, быть позитивными). Тогда каждому объекту оценки соответствует точка в двухмерном пространстве, показывающая соответствие уровней качества оцениваемой и базовой продукции по расположению в определенных частях поля [30, с. 67]. Применение квалиметрических методов построения, измерения и оценки показателей качества к категории эффективности инноваций как совокупности необходимых свойств позволяет решить задачу комплексного измерения эффективности инноваций, на основании чего осуществляется выбор наиболее эффективных.

Измерение параметров комплексной оценки эффективности инноваций производится с помощью экспертных технологий. Анализ типовых задач, решаемых методом экспертных оценок [23, 28, 29], показал, что выбор наиболее эффективных инноваций представляет собой задачу разработки альтернативных вариантов принятия решений в определенной ситуации с оценкой их предпочтительности.

Применительно к выбору инноваций целесообразно использовать оценочные анкеты, в которых присутствуют специальные графы, в которых дается оценка инноваций по тем или иным критериям по оговоренной шкале. Оценки могут даваться в качественной форме или количественной в виде интервалов (диапазона значений). Для количественной обработки оценочной информации лучше применять анкеты закрытого типа, в которых для каждого вопроса даются несколько вариантов ответа, отражающих ту или иную точку зрения и которым в последующем можно присвоить баллы или коэффициенты.

Для определения альтернативных вариантов решения задачи и принятия решений с оценкой их предпочтительности наиболее часто используются методы «Дельфи» и мозговых атак. Метод «Дельфи» – это инструмент проведения групповых экспертиз на основе процедур, объединенных общими требованиями к организации экспертизы и форме получения количественных экспертных оценок.

Преимущество метода «Дельфи» состоит в обратной связи, позволяющей экспертам корректировать свои суждения с учетом промежуточных усредненных оценок и пояснений экспертов, высказавших «крайние» точки зрения (диссидентов). Для этого экспертиза проводится в несколько туров (этапов). Статистическая обработка результатов анкетирования дает возможность не только оценить степень согласованности мнений экспертов, но и скорректировать программу опроса (анкету), что позволяет получить более достоверную оценку экспертизы.

Преимущества метода «Дельфи» состоят в анонимности, обеспечиваемой применением анкет (вопросников) для индивидуального опроса; регулируемой обратной связи, осуществляемой за счет проведения опроса в несколько этапов с сообщением результатов экспертам для возможной корректировки их оценок; истинности групповых оценок, характеризуемых однородностью ряда

индивидуальных оценок и приемлемым для обоснованных статистических выводов уровнем их вариации.

Для выбора приоритетных направлений инновационного развития и инноваций можно использовать метод мозгового штурма, относящийся к эвристическим методам исследования систем управления. Для решения поставленной задачи метод мозгового штурма целесообразен при разработке первоначального списка инноваций, который включает не только готовые к производству и реализации инновации, но и новации на стадиях открытий, изобретений, прикладных исследований.

Комплексный подход к оценке эффективности инновационных направлений развития или внедрения инноваций не означает ухода от сущности категорий «эффект и эффективность», параметров их оценки. Он состоит в сопоставлении комплексных оценок результатов и затрат на внедрение инновационных объектов, полученных в ходе экспертного оценивания отбираемых из множества альтернатив. Для комплексного сопоставления сложно формализуемых результатов внедрения инноваций и затрат на их внедрение российскими учеными был предложен ***экспертно-квалиметрический метод*** **(*ЭКМ*),** позволяющий произвести экспертную количественную оценку эффективности инноваций по определенной системе показателей и процедур [11, 19, 27, 32].

Предлагаемый экспертно-квалиметрический подход расширяет методологию оценки эффективности инновационных проектов, добавляя к динамическим и статическим показателям эффективности инновационных проектов экспертно-квалиметрические и ранговые оценки эффективности инновационных объектов, к стоимостным методам измерения эффективности качественные. Адаптация ЭКМ к специфике инфокоммуникаций позволит адекватно решить проблему выбора эффективного инновационного решения или наиболее эффективной инновации из множества альтернатив с учетом комплекса воздействующих факторов.

Сущность экспертно-квалиметрического метода и его применение для выбора эффективных инноваций

Экспертно-квалиметрический метод (ЭКМ) выбора эффективных инноваций представляет собой совокупность способов и приемов получения экспертами количественной оценки эффективности инноваций по определенной системе процедур и выбора наиболее эффективных из совокупности альтернатив. В основе этого метода лежит рассмотрение эффективности как совокупности свойств, отражающих отдельные проявления эффектов и барьеров внедрения инноваций, которые оценивают эксперты в количественной форме (в баллах), и комплексная форма выражения эффективности, уровень которой служит критерием выбора наиболее эффективных инноваций [11, 33]. Этот метод позволяет получить комплексную оценку эффективности инноваций на основе экспертного оценивания и обоснованно выбрать эффективные инновации из множества альтернативных вариантов.

Экспертно-квалиметрическая оценка эффективности инноваций дает возможность проводить сравнительную оценку не одного, а множества инновационных проектов, из которых осуществлять выбор наиболее эффективных вариантов с учетом потребительского спроса и производственных возможностей операторов связи. Экспертно-квалиметрический метод включает установление ранга альтернативных вариантов инноваций на основе комплексного показателя эффективности по совокупности индикаторов, отражающих различные эффекты [11, 19].

Цель разработки экспертно-квалиметрического подхода состоит в формировании средств и методов обоснования выбора наиболее эффективных инноваций на первых этапах жизненного цикла, когда отсутствует количественная информация о результатах и последствиях внедрения множества инноваций.

В основе экспертно-квалиметрического подхода к выбору эффективных инноваций лежит рассмотрение эффективности как совокупности отдельных свойств, отражающих отдельные проявления эффектов и барьеров внедрения инноваций, которые оценивают эксперты в количественной форме (в баллах), и комплексная форма выражения эффективности, уровень которой служит критерием выбора наиболее эффективных инноваций.

Основными процедурами экспертно-квалиметрического подхода к выбору эффективных инноваций являются:

- экспертное оценивание посредством количественного выражения мнений экспертов о потенциально-возможных результатах и затратах внедрения инноваций;
- комплексная оценка эффективности инноваций по совокупности условий и факторов их реализации;
- расчет коэффициентов эффективности и ранжирование инновации по его уровню с выделением наиболее эффективных.

Для проведения процедуры экспертного оценивания и оценки эффективности инноваций необходимо методологическое обоснование качества экспертов, анкет, шкал оценивания, частных и обобщающих показателей эффективности, способов построения комплексных показателей и их наглядного представления. Методологической базой экспертно-квалиметрического подхода к выбору эффективных инновации являются методы экспертной оценки [23, 28, 29] и квалиметрические методы построения на их основе обобщающих показателей эффективности, имеющих параметрический, но не всегда стоимостной характер [23, 25, 26, 31].

Важной методологической задачей является обоснование частных и обобщающих показателей эффективности инноваций с учетом затрат на их создание и реализацию, методов измерения, анализа и обработки данных с учетом неполноты информации и специфики экспертных оценок, характеризующих предвидение уровней и динамики результатов и затрат по отдельным инновациям или их совокупности.

Рассмотрим кратко сущность и процедуры реализации экспертно-квалиметрического метода в сфере инфокоммуникаций. Для идентификации

различных проявлений эффектов/барьеров внедрения инноваций в сфере инфокоммуникаций с индикаторами и показателями эффективности в монографии [19, с. 179] была первоначально составлена таблица 1, на основе которой в обобщенном виде определено содержание комплексной оценки эффективности инноваций (рис. 4).

Таблица 1 – Показатели эффективности инфокоммуникационных инноваций

Эффекты / Барьеры	Индикатор	Показатель
Результативная составляющая		
Увеличение перечня услуг и спроса, производственных мощностей, удовлетворение новых потребностей в услугах и технологиях	Потенциальный рост объема рынка продаж, доходов от услуг, абонентской базы, трафика, качества услуг.	Темпы прироста доходов (абонентов)
Переход к новым услугам и технологиям, резкое изменение потребностей и спроса, конкурентное преимущество.	Прорывный характер внедрения – рост масштабов производства и потребления	Увеличение доли рынка
Внедрение прогрессивных технологий, экономия материальных ресурсов и электроэнергии, рост быстродействия оборудования, прирост прибыли за счет экономии издержек	Рост производительности труда, снижение материалоемкости и себестоимости услуг	Прирост прибыли за счет снижения себестоимости услуг
Затратная составляющая		
Технологическая сложность внедрения нового оборудования (технологий, стандартов) вследствие технической и организационной сопряженности с действующими сетями и оборудованием, требующая модернизации базовой сети, создания новой сети доступа и сервисного обслуживания	Соизмеримость общих затрат на внедрение инноваций на сети связи с затратами на новое оборудование (технологии, стандарты)	Превышение общих затрат на внедрение над стоимостью нового оборудования
Воздействие микро и макроэкономических факторов риска в процессе создания и внедрения инноваций. Неготовность рынка к восприятию инновации и оператора к ее реализации	Возможность отрицательных последствий внедрения инноваций	Риск – степень вероятности упустить выгоду или понести убытки, отсутствия потребности на рынке
Экономическая сложность создания и внедрения инноваций с учетом сопряженных затрат на модернизацию сетей, лицензирование деятельности, приобретение частотного ресурса	Соизмеримость стоимости и результатов внедрения инноваций	Превышение общих затрат на внедрение над выручкой

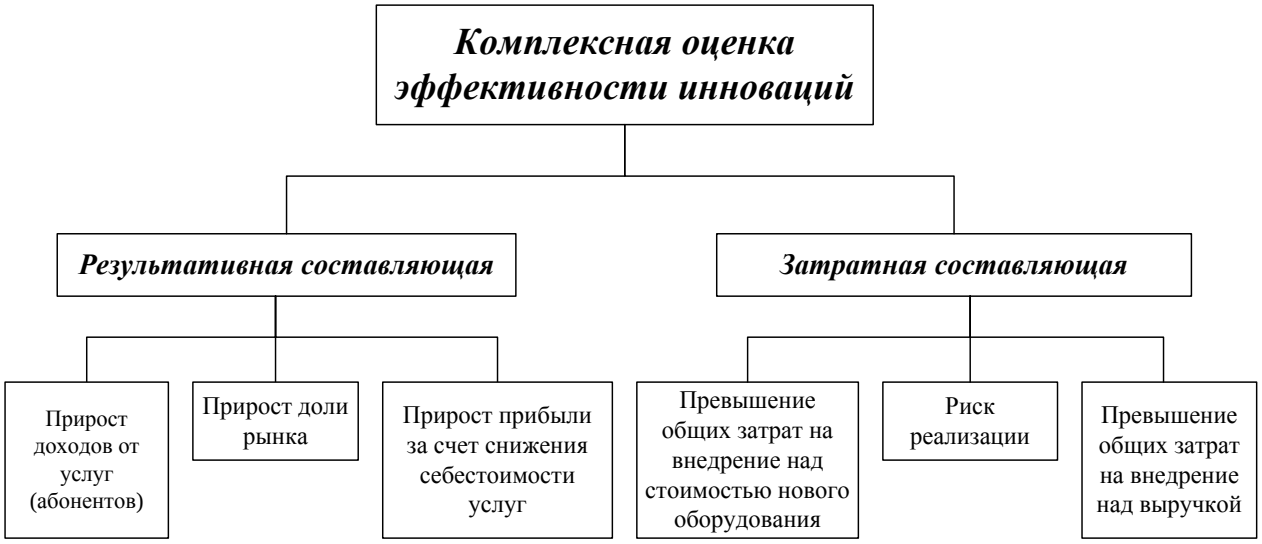


Рис. 4. Система показателей комплексной оценки эффективности инноваций в сфере инфокоммуникаций

Результативная составляющая эффективности инноваций должна отражать эффекты от внедрения инноваций на рынке в сфере инфокоммуникаций, другими словами эффекты увеличения объемов и качества услуг, роста потребностей пользователей, перехода к новым технологиям производства услуг, экономии материальных ресурсов и электроэнергии, быстродействия, миниатюризации и других эффектов научно-технического прогресса. Рост производственной мощности выражается ростом объема оказываемых услуг, доходов, абонентов, трафика, капитализации.

Внедрение инноваций ресурсосберегающего характера и прогрессивности технологий способствует росту производительности труда, снижению материалоемкости и энергоемкости, себестоимости и, в конечном счете, увеличению прибыли за счет снижения издержек производства услуг. Причем, если новая инновационная технология или услуга имеет прорывной, революционный характер внедрения, то ее рыночный потенциал может быть оценен существенным изменением масштаба производства и потребления, т.е. ростом доли компании на рынке.

Затратная составляющая эффективности инноваций отражает высокие затраты ресурсов, технологическую сложность создания и внедрения инноваций, уровень рисков их реализации как совокупность барьеров ресурсно-затратного характера. С учетом специфики инфокоммуникаций затратность инноваций выражается не только затратами на создание самих инноваций (стоимость), но и технологической сложностью их реализации вследствие необходимости обеспечения технической и организационной сопряженности с действующими сетями и оборудованием, т.е. затратами на модернизацию сетей при их внедрении (общие затраты). Кроме того, внедрение инноваций сопровождается значительными рисками как их производства, так и реализации на достаточно насыщенном рынке инфокоммуникационных услуг и оборудования.

Оценка риска реализации как вероятности понести убытки при выборе неэффективного инновационного решения или упустить выгоду от внедрения неэффективной инновации, в значительной мере обеспечивает гарантию принятия обоснованных инновационных решений. При внедрении инноваций возникает множество взаимодействующих и взаимосвязанных рисков финансирования инвестиций, поведения конкурентов и потребителей, политики государства, форс-мажорных обстоятельств, поэтому оценка рисков имеет интегральный характер.

На основе результатов экспертного оценивания инноваций путем выставления балльных оценок по параметрам результативной и затратной составляющих эффективности инноваций с учетом их значимости появляется возможность произвести количественную (квалиметрическую) комплексную оценку эффективности инноваций по коэффициенту эффективности инноваций:

$$K_{ЭИ} = \frac{P_И}{З_И} = \frac{a_{1j}\Delta Q + a_{2j}\Delta d_r + a_{3j}\Delta П_C}{b_{1j}C_{ТИ} + b_{2j}R_И + b_{3j}C_{ЭИ}}, \quad (2)$$

где $P_И$ - результативная составляющая эффективности инноваций определяется как функция от переменных: потенциальный прирост доходов от услуг связи ΔQ, прирост рыночной доли или прорывной рыночный потенциал Δd_r, прирост прибыли за счет снижения себестоимости услуг $\Delta П_C$:

$$P_И = f(\Delta Q, \Delta d_r, \Delta П_C); \; P_И = a_{1j}\Delta Q + a_{2j}\Delta d_r + a_{3j}\Delta П_C;$$

где $З_И$ - затратная составляющая эффективности инноваций определяется как функция от переменных: технологическая сложность (превышение общих затрат на внедрение над стоимостью нового оборудования) $C_{ТИ}$, риск реализации $R_И$, соизмеримость стоимости и результатов внедрения инноваций (превышение общих затрат на внедрение над выручкой) $C_{ЭИ}$:

$$З_И = f(C_{ТИ}, R_И, C_{ЭИ}); \; З_И = b_{1j}C_{ТИ} + b_{2j}R_И + b_{3j}C_{ЭИ};$$

где a_{ij}, b_{ij} - коэффициенты значимости показателей результативной и затратной составляющих эффективности инноваций; i - число показателей составляющих эффективности (в данном случае i=1÷3); j - число групп (кластеров) инноваций в зависимости от вида связи, положения на сети связи, типа инноваций (услуги, оборудование, технология) и т. д. (j = 1÷7).

Соотношение суммарных средневзвешенных оценок в баллах результативной и затратной составляющих эффективности инноваций дает количественное выражение оценки в виде коэффициента. Если коэффициент эффективности инноваций $K_{ЭИ}$ много больше единицы ($K_{ЭИ}$>1,5), то эффективность внедрения инноваций очень высокая; если 1<$K_{ЭИ}$<1,5, то – высокая; если 0,8<$K_{ЭИ}$<1, то – средняя; если 0,5<$K_{ЭИ}$<0,8, то низкая, если $K_{ЭИ}$ < 0,5, то очень низкая. Инновации с очень низкой эффективностью не включаются в перечень выбранных эффективных инноваций и не принимают участие в ранжировании. Аргумент принятия такого решения состоит в несоответствии эффекта и затрат на внедрение инновации: затраты в 2 раза и более превышают результат.

Методическое обоснование параметров и процедуры экспертного оценивания эффективных инноваций

Квалиметрический метод построения интегрального показателя эффективности инноваций в сочетании с экспертным методом оценки его параметров позволяет осуществлять прямое их ранжирование по уровню эффективности, что является особенно важным при принятии стратегических или тактических решений по инвестированию инновационных разработок или покупке новых технологий, систем, оборудования в сфере инфокоммуникаций.

Основным критерием оценки согласованности мнений экспертов по выбору инноваций в соответствии с методом «Дельфи» являются коэффициенты вариации экспертных оценок (в баллах) совокупности исследуемых инноваций. Размеры коэффициентов вариации по всем эффективным инновациям, включая инновации с очень низкой эффективностью, которые не вошли в перечень эффективных инноваций, должны находиться в пределах 15-20%, то есть в пределах однородной совокупности мнений экспертов [28].

Для оценки согласованности мнений экспертов об эффективности всей совокупности инноваций используется коэффициент вариации, который рассчитывается на основе средневзвешенных баллов оценок, выставленных отдельно по результативной и затратной составляющим эффективности и по коэффициентам эффективности инноваций:

$$V_j = \frac{\sigma_j}{C_j};\ \ \overline{C}_j = \frac{\sum_{i=1}^{m} C_{ij}}{m};\ \ \sigma_j = \sqrt{\frac{\sum (C_{ij} - \overline{C_j})^2}{m}}, \qquad (3)$$

где C_{ij} - оценка результативной (затратной) составляющих эффективности и оценка коэффициента эффективности, данные *i*–тым экспертом *j*–той инновации; $\overline{C_j}$ - средняя арифметическая оценок результативной (затратной) составляющих эффективности и коэффициента эффективности, данных экспертами по *j*–той инновации; σ_j - среднее квадратическое отклонение оценки *j*–той инновации; *m* - число экспертов.

Методическое обоснование аппарата комплексной оценки эффективности инноваций кроме обоснования частных показателей результативной и затратной составляющих эффективности, отражающих наиболее значимые индикаторы эффектов/барьеров внедрения инноваций, и построения интегрального показателя в форме соотношения обобщающих показателей, отражающих результаты и затраты на внедрение инноваций в количественном выражении, включает две важнейшие процедуры:

- определение адекватных каждому из частных показателей шкал измерения для получения однозначного вывода об эффективности;
- установление значимости (весомости) частных показателей в результативной и затратной составляющих эффективности с учетом кластеризации инноваций по сферам деятельности.

В квалиметрии и экспертном оценивании шкала используется как метод оценивания и сопоставления свойств различных объектов или характеристик изучаемого явления [28]. Поскольку шкала отношений применима к большинству параметров экономической оценки и при ее использовании возможны арифметические действия, то мы воспользуемся ею для непосредственной оценки индикаторов эффективности инноваций в баллах. Балльная шкала оцениваемых свойств продукции, конкурентоспособности, эффективности служит для назначения оцениваемому свойству количественных характеристик, являющихся мерой этих свойств.

Для оценивания сразу шести частных показателей результативной и затратной составляющих эффективности инноваций требуется комплексный подход, состоящий в малом количестве градаций в баллах (1, 2 и 3 балла, соответствующих низкому, среднему и высокому эффекту или барьеру) и наборе количественных диапазонов изменения частных индикаторов эффективности. Такой подход позволяет эксперту однозначно устанавливать соответствие оценки в баллах индикатору эффективности.

При формировании количественных диапазонов изменения частных показателей эффективности следует учитывать, что эксперту не обязательно знать, как рассчитывается показатель и каковы его стоимостные характеристики в каждом конкретном случае. Задача экспертного оценивания состоит в четком и однозначном установлении соответствия величины балла шкале оценивания, то есть низкому, среднему и высокому уровню изменений или характеристик частных показателей эффективности.

Для установления диапазонов шкалы по различным показателям эффективности инноваций был проведен анализ изменения важнейших экономических показателей основных инфокоммуникационных компаний, функционирующих на развитых и развивающихся сегментах рынка [11]. На развитых сегментах инфокоммуникационного рынка с высоким уровнем проникновения услуг связи и доступности средств связи рыночный потенциал, риск и сложность реализации оказываются существенно ниже, чем на развивающихся региональных сегментах рынка. Это определяется высокими затратами на формирование инфраструктуры (базовых сетей, сетей доступа) при высоких темпах роста региональной абонентской базы и доходов.

Полученные диапазоны вариации индикаторов эффективности деятельности операторов связи, существенно различающиеся по рыночной ситуации, свидетельствуют о необходимости учета экспертами характера изменения параметров оценки эффективности внедрения инноваций. Для выделения наиболее характерных диапазонов изменения частных показателей эффективности экспертной группе (43 чел.) были даны разные варианты шкал оценивания. Результаты экспертной оценки целесообразных диапазонов шкал оценивания частных показателей эффективности показали, что из нескольких диапазонов большинство экспертов (более 80%) поддерживает по каждому кластеру инноваций один, что послужило основой установления шкал или диапазонов изменения частных показателей.

Обоснованные индикаторы имеют разную значимость или вес в оценке эффективности инноваций разных кластеров инноваций. Поэтому возникает задача установления экспертами весомости, значимости частных показателей результативной и затратной составляющих эффективности инноваций с учетом их кластеризации по сферам деятельности или сферам применения. Количественная оценка значимости индикаторов эффективности инноваций по различным кластерам была установлена на основе структуры экспертов, поддержавших вес частных показателей в разрезе обобщающих показателей эффективности инноваций.

Величина значимости индикаторов устанавливалась по удельному весу экспертов, отдающих предпочтение тому или иному индикатору в разрезе результативной и затратной составляющих:

$$a_i = \frac{k_i}{\sum_{i=1}^{3} k_i} \cdot 100\,(\%), \qquad (4)$$

где k_i - количество экспертов, отдающих предпочтение по значимости i-му индикатору результативной или затратной составляющих эффективности; i=1÷3; $\sum a_i = 100\%$. Округление значимости индикаторов эффективности производится до десятых долей или десятков процентов.

Анкета по оценке эффективности инноваций имеет форму таблицы, в строках которой указывается краткое описание инновации, эффекты их внедрения, в графах – показатели результативной и затратной составляющих эффективности с указанием диапазонов шкалы измерения и место для балльной оценки. Простота изложения вопросов и однозначность ответов позволяют обеспечить достоверность результатов экспертизы и возможность оперативной обработки результатов.

При разработке вопросника были учтены теоретические положения по анкетированию [28, 34], требования к анкетам и вопросам, типы анкет, шкалы ответов. Чтобы вопрос был однозначным и сконцентрирован на одной проблеме в анкете должна даваться аннотация, то есть краткое описание сущности технологии, технических характеристик, сферы использования инновации, а также принадлежность к кластеру по сфере деятельности. Чтобы вопрос был понятен эксперту, являлся однозначным и количественно измеряемым, в ответах была предусмотрена расшифровка ответов с соответствующим уровнем баллов. Поскольку анкета классифицирована по сферам деятельности – кластерам инноваций, то это позволяет аналитической группе сразу сгруппировать результаты экспертного оценивания по сегментам бизнеса. Краткое описание инновации в анкете позволяет экспертам давать однозначные ответы и балльную оценку для количественного измерения мнений экспертов и оценки их согласованности.

Для получения достоверных результатов отбора эффективных инноваций проводится оценка степени согласованности мнений экспертов. Анализ и обсуждение существенных отклонений в оценках экспертов по индикаторам эффективности позволяют уточнить параметры анкеты или компетентность

экспертов в вопросах оценки эффектов и препятствий (сложности) реализации инноваций.

Наличие возможности рассмотрения экспертами результатов экспертизы и уточнения параметров экспертных заключений, включая мнение эксперта, реализуемых методом «Дельфи» в условиях количественных оценок индикаторов составляющих комплексной оценки эффективности, позволяет при одно- двухтуровой экспертизе получить достоверные оценки эффективности и ранжировать инновации по уровню эффективности.

Наиболее ответственным этапом выбора инноваций является формирование экспертной группы. Однако для включения в экспертную группу по выбору наиболее эффективных инноваций высокого профессионализма недостаточно, необходимы люди перспективного типа мышления, системно оценивающие результаты НТП и обладающие внутренней способностью предвидения будущих технологий связи, основанной на нетривиальных способах решения [28, с. 31].

Для определения качества экспертов используются априорные, апостериорные и тестовые методы оценки [28]. Одним из априорных методов является самооценка экспертом своих качеств: компетентности, креативности, конформизма, аналитичности, широты мышления и самокритичности, по балльной, числовой и вербальной шкалам или на основе коэффициента компетентности.

Для формирования экспертной группы должна проводиться самооценка экспертов по балльной шкале, а на основе коэффициентов компетентности – характеристика качества экспертов. Экспертам предлагалось оценить себя по двум параметрам: информированности по проблеме и степени аргументации в основе знакомства с источником информации в различных и профессиональных областях: инфокоммуникации, фиксированные и беспроводные широкополосные технологии/услуги, проектирование и планирование развития сетей связи, маркетинг и стратегия продаж, бизнес - планирование, экономика и финансы, инновационный менеджмент, стратегия развития внешних и внутренних рынков инфокоммуникационных услуг, стратегия корпоративного развития. В перечисленных областях профессиональной деятельности эксперты должны были оценить свою информированность и степень аргументации по пятибалльной шкале.

Коэффициент компетентности эксперта $K_{комп}$ определяется как средняя из коэффициентов информированности по проблеме $K_{инф}$ и коэффициента аргументации $K_{арг}$, отражающих источники информированности, знаний и аргументации. Совокупная самооценка компетентности эксперта $K_{комп}$ определяется с учетом оцениваемых областей знания (n) по формуле:

$$K_{комп} = \frac{1}{2 \cdot n} \sum_{i=1}^{n} (K_{инф} + K_{арг}), \quad (5)$$

где $K_{инф}$ - коэффициент информированности по проблеме, отражающий источники информированности и знаний; $K_{арг}$ - коэффициент аргументации, отражающий теоретические знания и производственный опыт; n - число оцениваемых областей знания.

Сводные результаты оценки качества группы экспертов (из 50 специалистов немецких и российских организаций) представлены в таблице 2.

Таблица 2 – Сводные результаты оценки компетентности экспертов

Iнтервалы оценок в баллах	от 1 до 2	от 2 до 3	от 3 до 4	От 4 до 5	Всего
Количество экспертов, чел.	0	7	23	20	50
Средняя оценка по совокупности, балл	-	2,81	3,65	4,74	3,97
Количество экспертов с оценкой более 3-х баллов	0	0	23	20	43
Средняя оценка по группе экспертов с оценкой более 3-х баллов	-	-	3,65	4,74	4,15

Анализ сводных и частных результатов самооценки компетентности экспертов в составе 50 человек показал их достаточно высокое качество – 3,97 балла. Результаты самооценки компетентности экспертов по установленным профессиональным областям знаний по пятибалльной шкале демонстрируют различие оценок по уровням информированности по проблеме и аргументации, а также совокупных коэффициентов компетентности. При этом наличие несистематизированных теоретических знаний (2 балла) и недостаточности источников аргументации (2 балла) для принятия решения по выбору эффективных инноваций послужило основанием для исключения экспертов с самооценкой компетентности менее 3-х баллов и установлению окончательной численности группы экспертов в 43 человека со средним уровнем компетентности в 4,15 балла, из них 18 человек – сотрудники немецких компаний, 25 – российских компаний.

Результаты оценки эффективности и выбора инноваций в сфере инфокоммуникаций

Проведенные исследования отечественных и зарубежных инноваций в сфере инфокоммуникаций методом технологического радара [10, 11, 19] позволили выделить из общего перечня наиболее актуальные инновации (192 ед.), которые и стали предметом апробации экспертно-квалиметрического метода для отбора наиболее эффективных инноваций с целью внедрения на инфокоммуникационном рынке.

На основе анкет опроса об эффективности инфокоммуникационных инноваций экспертная группа осуществила экспертное оценивание, выставив оценки в баллах по каждому частному показателю результативной и затратной составляющих эффективности. Обработка результатов производилась по группам (кластерам) инноваций, соответствующим сферам деятельности и применения, и в целом по совокупности эффективных инноваций.

Использование совокупности показателей эффективности с разными диапазонами шкал оценивания обусловили более жесткую процедуру

экспертного оценивания при достаточно высоком уровне согласованности мнений экспертов. Сводные результаты экспертного оценивания инфокоммуникационных инноваций по коэффициенту эффективности свидетельствуют о том, что перечень эффективных инноваций (65 ед.) значительно меньше перечня актуальных инноваций (192 ед.).

Обобщение результатов экспертного оценивания инноваций на основе экспертно-квалиметрического подхода, представленной в таблице 3, показывает, что общий уровень эффективности актуальных инноваций весьма низок – 0,69 (в пределах от 0,5 до 0,8 коэффициента эффективности). Средний уровень коэффициента эффективности эффективных инноваций составляет 1,22. Это означает, что общий уровень эффективности инноваций в сфере инфокоммуникаций высокий и обеспечивает превышение уровня результативной составляющей над затратной. Другими словами, эффективные инновации обеспечивают превышение эффектов рыночного потенциала (роста объемов продаж, прибыли, доли рынка) над технологической и экономической сложностью внедрения инноваций на рынке.

Таблица 3 – Характеристика средних экспертных оценок и показателей вариации по совокупности актуальных и эффективных инноваций

Инновации	Количество	Результативная составляющая		Затратная составляющая		Коэффициент	
		Средний балл	Коэффициент вариации, %	Средний балл	Коэффициент вариации, %	Эффективности, отн.ед.	Вариации, %
Актуальные	192	1,56	14,8	2,19	16,3	0,69	15,4
Эффективные	65	2,18	10,7	1,79	11,1	1,22	10,9

Размеры коэффициентов вариации по всем актуальным инновациям, включая инновации с очень низкой эффективностью, которые не вошли в перечень эффективных инноваций, находятся в пределах 15-20%, то есть в пределах однородной совокупности мнений экспертов.

Средний уровень согласованности мнений экспертов по актуальным инновациям по результативной составляющей составил 14,8%, по затратной – 16,3%, по коэффициенту эффективности – 15,4%, что свидетельствует о достаточно высоком качестве экспертов по уровню компетентности и достаточно высоком уровне качества анкет. Величины средних уровней коэффициентов вариации по эффективным инновациям еще ниже и находятся в пределах 10-11%, что указывает на высокую достоверность результатов экспертного оценивания и возможность проверки гипотезы о нормальном распределении полученных оценок эффективности и использовании средних коэффициентов эффективности в качестве типичных характеристик отобранных инноваций.

Для оценки близости эмпирического распределения коэффициентов эффективности, полученных экспертами в ходе экспертизы инноваций по критерию эффективности, теоретически нормальному распределению можно использовать критерии согласия К. Пирсона χ^2 (хи-квадрат), А.Н. Колмогорова λ и др. [35, с. 253-255].

Расчеты показывают, что расчетное значение $\chi^2_{расч}=2,915$. При степени свободы, равном 3, и уровне значимости 0,05 табличное значение критерия $\chi^2_{табл}=7,815$. Поскольку $\chi^2_{расч}< \chi^2_{табл}$, то с вероятностью 0,95 фактическое распределение близко к теоретически нормальному. Таким образом, распределение коэффициентов эффективности, полученных в ходе экспертной оценки инноваций, соответствует закону нормального распределения.

Этот вывод подтверждается расчетом критерия согласия Колмогорова $\lambda=4,9/\sqrt{65}= 0,608$. При $\lambda = 0,6$ вероятность $P(\lambda)=0,864$, то есть с вероятностью 86,4% можно говорить о близости фактического и теоретически нормального распределений.

По результатам отбора экспертами наиболее эффективных инноваций в соответствии с величинами коэффициентов эффективности можно судить о ***тенденциях в инновационном развитии инфокоммуникаций***:

- большинство инноваций с коэффициентом эффективности более 2,0 отражает развитие сетей нового поколения с широким спектром технических и пользовательских возможностей, конвергенцию фиксированных и мобильных сетей, цифровизацию телевидения на всех сетях и применение в сетях IP-протокола (NGN, IMS, All IP networks, IPTV, MPLS, SIP Service, Multi Play, Multi Mode Mobile Phones);
- инновации с коэффициентом эффективности в пределах 1,0 отражают степень развития современных сетей сотовой связи (GSM/GPRS, 4G), сетей беспроводного широкополосного доступа, фиксированных сетей передачи данных (проводных/кабельных) и телефонных сетей общего пользования;
- инновации с низким уровнем эффективности не способны значительно увеличить доходы операторских компаний, поддерживать устойчивый рост их доходов, поскольку имеют либо косвенное отношение к деятельности компаний (терминалы), либо представляют собой инновации, использование которых не может контролировать оператор (например, самоорганизующиеся mesh-сети, USB-накопители с самоактивируемыми приложениями). Внедрение этих инноваций может стимулировать рост трафика в сетях операторов связи.

В результате комплексной оценки эффективности актуальных инноваций было отобрано 65 эффективных. Очень высокий экономический эффект следует ожидать от внедрения 15 инноваций (23,1% от общего числа рассматриваемых инноваций), высокий – от 32 инноваций (49,2% инноваций), средний – от 10 инноваций (15,4%) и невысокий экономический эффект - от 8 инноваций (12,3% инноваций).

Структура эффективных инноваций по кластерам, приведенная на рис. 5, свидетельствует о том, что эксперты отдали приоритет инновациям в сфере сетей доступа (30%), услуг конечному пользователю (23%) и базовой сети (15%), что подтверждает стратегические направления инновационного развития инфокоммуникаций – формирование перспективной и надежной инфраструктуры для завоевания рыночных сегментов и более полного удовлетворения потребностей клиентов.

Группировка эффективных инноваций по этапам жизненного цикла (рис. 6) показала, что эксперты при оценке экономической целесообразности склонились в пользу инноваций, представленных на мировых телекоммуникационных рынках (40%) или прошедших стадию образца – рыночного прототипа (28%), не оставив без внимания создаваемые инновации на этапах концепций, идей (19%) и прикладных исследований (13%).

Такое распределение инноваций характерно для компаний связи, которые производят услуги и совершенствуют производство за счет приобретения готовых продуктов и технологий, на основе которых обеспечиваются доходность и конкурентные преимущества. Наименьший интерес для компаний представляют инновации, находящиеся в стадии «исследования». Это обусловлено большим временным интервалом между стадиями «исследования» и «наличие на рынке», за время которого инновация может потерять свою актуальность в условиях высокой динамичности развития телекоммуникационного рынка.

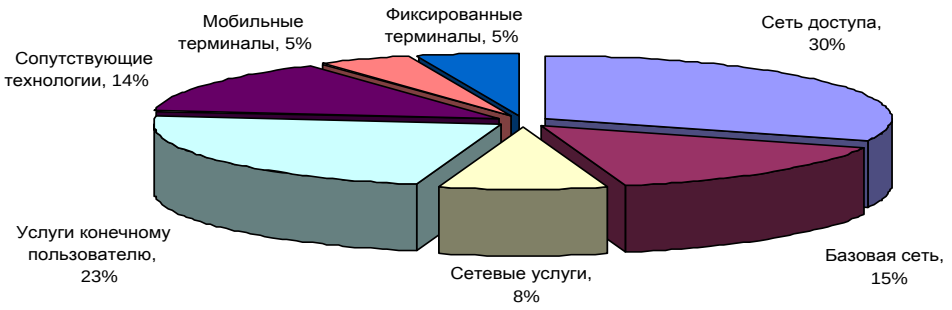


Рис. 5. Распределение эффективных инноваций по кластерам

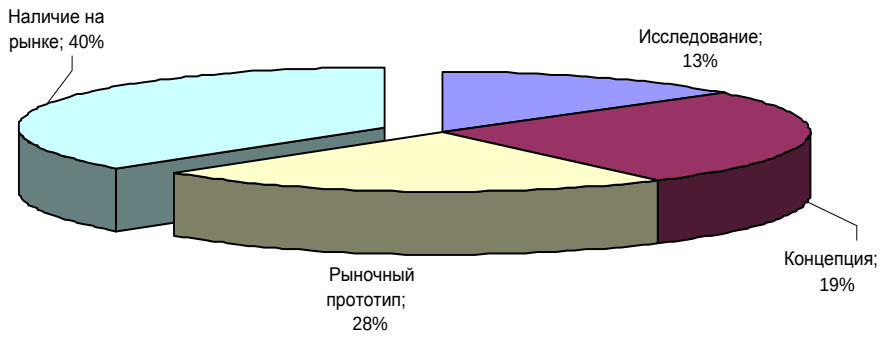


Рис. 6. Распределение эффективных инноваций по этапам жизненного цикла

Большое количество актуальных инновационных технологий и услуг относятся к сегменту «сеть доступа», что обусловлено повышающимися

требованиями к мобильности пользователей, абонентского терминала и обслуживания. Наибольшее число эффективных инновационных решений находится в кластере базовых сетей, что подчеркивает важность и перспективность конвергенции сетей фиксированной и мобильной связи, развития инфраструктуры глобальных сетей нового поколения, обеспечивающих высокоскоростную широкополосную передачу данных, управление качеством передачи данных, IP технологий и предоставление мультисервисных услуг.

Интегрально-экспертный подход к комплексному измерению эффективности применения инфокоммуникационных технологий

Формирование модели интегральной оценки эффективности применения инфокоммуникационных технологий (ИКТ) и развития инфокоммуникаций с учетом множества влияющих факторов, синергетического эффекта и негативных последствий информатизации основывается на научных подходах к формированию интегральных показателей, отборе наиболее адекватных поставленной задаче методов и разработке методического инструментария обеспечения экспертной оценки эффективности применения ИКТ и развития инфокоммуникаций во взаимосвязи с формированием информационного общества [36, 37].

Применение экспертно-квалиметрического подхода, методов исчисления комплексных показателей и технологии экспертного опроса эффективности применения ИКТ с оценкой значимости обобщающих показателей и целесообразности введения в модель частных показателей с учетом положительных и отрицательных эффектов последствий информатизации и применения ИКТ дают основание для формирования модели интегрального показателя эффективности применения ИКТ в форме относительного коэффициента эффективности как соотношения интегральных результативных и затратных показателей, взвешенных по весу экономической и социальной компонент эффективности [38].

В условиях бурного развития научно-технического прогресса в сфере инфокоммуникаций, углубления конвергентных процессов относительно технологий, услуг, сетей и бизнеса различных секторов экономики, повышения активности позиций пользователей в восприимчивости новых услуг и технологий происходит широкомасштабное проявление новых качественных параметров эффективности ИКТ. При высокой значимости экономической оценки эффективности внедрения ИКТ не менее ценными является социальный эффект [39].

По мере массового внедрения ИКТ и усиления влияния процессов информатизации на экономику и общество в целом происходит переосмысление теоретических концепций, отражающих данные события, выявляются их противоречивый характер и неоднозначные социально-экономические последствия. С одной стороны, прогресс выражается в росте производительности и интеллектуальности труда, повышении спроса на знания и ИКТ, увеличении свободного от производственной деятельности времени,

развитии «человеческого» и «социального» капитала общества, снижении промышленных рисков и технологических катастроф.

С другой стороны, развитие ИКТ коренным образом трансформирует современную экономику и общественную жизнь на основе формирования «электронного правительства», «электронного образования», «электронной медицины» и др., вызывает «информационную асимметрию», «информационное неравенство», привносит принципиально новые риски (кибернетические, информационные), кибер терроризм и необходимость обеспечения информационной безопасности.

Анализ международных и национальных показателей, оценивающих движение к информационному обществу, процессов эволюции параметров развития инфокоммуникаций и характера проявления эффектов применения инфокоммуникационных технологий (ИКТ) в экономической и социальной жизни позволил нам систематизировать факторы по характеру и направленности проявления эффективности, что стало основой создания адекватной комплексной системы показателей развития инфокоммуникаций и формирования информационного общества [40].

Проведенная нами систематизация факторов, влияющих на экономическую и социальную эффективности развития инфокоммуникаций, применение ИКТ и формирование информационного общества, представленная на рис. 7, указывает на наличие и необходимость модернизации системы измерения эффективности данных процессов в направлении учета как положительного, так и отрицательного эффектов.

Предложения международного партнерства по измерению ИКТ в целях развития информационного общества показали, что в мировом сообществе ключевым элементом характеристики состояния и развития инфокоммуникаций являются доступность ИКТ, масштабы и эффективность их использования в предпринимательском секторе, органах государственной власти, в социальной сфере, в домохозяйствах и населением.

При этом в современном обществе под инфокоммуникационными технологиями (ИКТ) понимают и инфраструктуру инфокоммуникаций и саму отрасль, и степень применения в конкретной деятельности, и Интернет и «электронное производство» и «электронное правительство» и т.д. Такая ситуация и принятый в обществе объединяющий характер понятия ИКТ обусловливают пристальное внимание к вопросам оценки происходящих процессов и измерения эффективности применения ИКТ [39].

Так как под эффективностью развития инфокоммуникаций во взаимосвязи с формированием информационного общества можно понимать, с одной стороны, степень использования возможностей инфокоммуникационной инфраструктуры и ИКТ для получения юридическими и физическими лицами экономического и социального эффекта, с другой стороны, – их готовность к использованию этих возможностей и жизнедеятельности в информационном обществе, то система показателей должна отражать процессы повышения эффективности деятельности и качества жизни людей, а также качественный переход национальной экономики к информационному обществу.

Рис. 7. Совокупность показателей факторов развития инфокоммуникаций и формирования информационного общества

Методическое обоснование аппарата комплексной оценки эффективности применения ИКТ и развития инфокоммуникаций и формирования информационного общества включает четыре важнейшие процедуры:

- обоснование частных показателей применения ИКТ и развития инфокоммуникаций, отражающих наиболее значимые экономические и социальные индикаторы положительных и отрицательных эффектов информатизации;
- построение моделей интегрального показателя на основе обобщающих показателей, отражающих положительные и отрицательные эффекты информатизации в количественном выражении;
- определение адекватных каждому из частных показателей шкал измерения для получения экспертами однозначного вывода об эффективности применения ИКТ и развития инфокоммуникаций;
- установление значимости (весомости) частных экономических и социальных показателей, отражающих положительные и отрицательные эффекты информатизации с учетом кластеризации по

сферам экономической деятельности, социальным группам и территориям потребления инфокоммуникационных технологий и услуг;
- построение моделей количественной оценки эффективности применения ИКТ и потенциала развития инфокоммуникаций во взаимосвязи с формированием информационного общества.

Таким образом, методологическое обоснование процедуры комплексной оценки эффективности применения ИКТ во взаимосвязи с формированием информационного общества предполагает не только обоснование показателей эффективности, отражающих экономические и социальные результаты и последствия внедрения ИКТ, методы обработки и представления результатов экспертного оценивания, но и формирование группы экспертов, разработку анкет опроса, их содержания, критериев отбора, шкал оценивания.

Комплексная система оценки эффективности применения ИКТ имеет иерархическую систему и включает два блока интегральных оценок, отражающих положительные эффекты и отрицательные последствия применения ИКТ и процессов информатизации (рис. 8). Интегральные результативный и затратный показатели эффективности применения ИКТ и развития инфокоммуникаций базируются на системе обобщающих и частных показателей экономической и социальной эффективности.

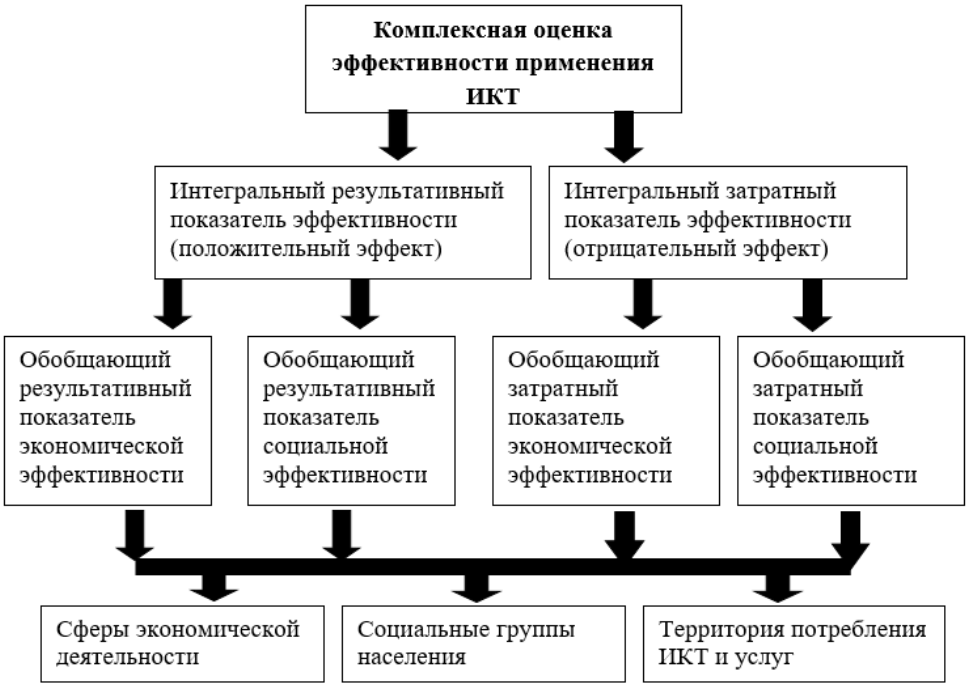


Рис. 8. Комплексная система оценки эффективности применения ИКТ

Методический аппарат интегральной оценки эффективности применения ИКТ во взаимосвязи с формированием информационного общества основан на применении экспертно-квалиметрического метода, разработанного для оценки эффективности инноваций и состоящего в получении количественных оценок эффективности посредством экспертного оценивания ее параметров [27, 32].

При разработке комплексной системы оценки эффективности развития инфокоммуникаций и формирования информационного общества важное значение имеет выбор ключевых частных показателей эффективности, с одной стороны, отражающих социально-экономические последствия информатизации, с другой стороны – степень охвата сфер экономической деятельности, социальных групп и территорий потребления инфокоммуникационных технологий и услуг.

Интегральные и обобщающие результативные и затратные показатели эффективности, в свою очередь, могут рассчитываться по результатам экспертного оценивания частных показателей на основе средней арифметической (простой, взвешенной) в абсолютном выражении (в баллах) или расчетных показателей в относительном выражении по методу нормированных отклонений или нормализованных величин.

Модель интегрального коэффициента эффективности применения ИКТ на основе баллов в абсолютном измерении имеет вид:

$$К_{эфф} = \frac{П_{инт.рез.}}{П_{инт.затр.}} = \frac{П_{об.р.эк.} \cdot d_{р.эк.} + П_{об.р.соц.} \cdot d_{р.соц.}}{П_{об.з.эк.} \cdot d_{з.эк.} + П_{об.з.соц.} \cdot d_{з.соц.}}$$

$$П_{об} = \sum_{i=1}^{n} П_i \cdot d_i \qquad (6)$$

где $К_{эфф}$ – интегральный коэффициент эффективности применения ИКТ и развития инфокоммуникаций (отн.ед.); $П_{инт.рез.}$, $П_{инт.затр.}$ – результативный и затратный интегральные показатели эффективности применения ИКТ и развития инфокоммуникаций; $П_{об.р.эк.}$; $П_{об.з.эк.}$ – обобщающие результативный и затратный показатели экономической эффективности; $П_{об.р.соц.}$; $П_{об.з.соц.}$ – обобщающие результативный и затратный показатели социальной эффективности; $П_i$ – i–тый частный показатель в разрезе обобщающих показателей; d_i – значимость i-того частного показателя; m – количество i-тых частных показателей; $П_j$ – j-тый частный показатель в разрезе кластеров исследования; d_j – значимость j-того кластера исследования; m - количество j-тых кластеров (виды экономической деятельности – отрасли экономики, социальные группы, территории потребления ИКТ услуг).

Алгоритм процедуры экспертного оценивания эффективности применения ИКТ и развития инфокоммуникаций во взаимосвязи с формированием информационного общества на основе интегрально-экспертного подхода представлен на рис. 9 и включает последовательность этапов анализа информации о характере эффектов и последствий экономического и социального характера, экспертной оценки эффективности и обработки результатов.

Рис. 9. Алгоритм процедуры экспертного оценивания эффективности применения ИКТ и развития инфокоммуникаций во взаимосвязи с формированием информационного общества на основе интегрально-экспертного подхода

Информационно-аналитический аппарат обоснования факторов и параметров модели интегральной оценки эффективности применения ИКТ и развития инфокоммуникаций реализуется на основе сбора экспертных данных о целесообразности включения тех или иных частных показателей в обобщающие и интегральный показатели; о величине значимости частных показателей в составе обобщающих компонентов интегральной оценки

экономической и социальной эффективности в разрезе положительных и отрицательных эффектов (затрат, последствий); статистической обработки информации, полученной методом экспертного опроса, включая анализ вариации мнений экспертов по совокупности частных показателей и оценку согласованности мнений членов экспертной группы; и интерпретации результатов оценки эффективности.

Практическое использование экспертно-квалиметрического подхода к комплексной оценке эффективности применения ИКТ и развития инфокоммуникаций предусматривает формирование параметров оценки эффективности, шкал их измерения и оценку их значимости с сохранением общего подхода к индикаторам по ЭКМ [11, 27, 32]. Вопросник заполняется экспертом с учетом положительных и отрицательных эффектов / барьеров экономического и социального характера, сопровождающих развитие инфокоммуникаций и формирование информационного общества. После ознакомления с частными показателями эффективности применения ИКТ эксперт дает оценку в баллах о целесообразности включения в модель интегральной оценки эффективности частных показателей эффективности в соответствии с трехбалльной шкалой оценки, их значимости – по 100% шкале и уровне эффективности по каждому частному показателю в разрезе обобщающих – по пятибалльной шкале. Самооценка эксперта производится по пятибалльной шкале.

По каждому показателю ставится только одна балльная оценка из трех/пяти позиций шкалы оценивания. При определении значимости частных показателей в составе обобщающих показателей эффективности следует иметь в виду, что сумма весов всех частных показателей должна быть равна 100%.

Результаты интегрально-экспертной оценки эффективности применения ИКТ в сфере инфокоммуникаций

Для определения практической приемлемости предлагаемой методики оценки эффективности применения ИКТ нами был проведен опрос семнадцати представителей инфокоммуникационных компаний, фактически использующих ИКТ (сеть Интернет, смартфоны, мобильные приложения, программные продукты) в производственной деятельности (производство услуг, обслуживание, администрирование) в 2016 году и оценки перспективной готовности использовать ИКТ и другие результаты развития инфокоммуникаций в 2020 году.

Сводные результаты самооценки экспертов по обоснованию состава показателей и оценке эффективности применения ИКТ приведены в таблице 4.

В целом коэффициент компетентности экспертов из кластера студенты по обоснованию показателей и оценке эффективности применения ИКТ достаточно высок и составляет 3,89 балла. Анализ приведенных данных свидетельствует о более высоком уровне качества экспертов по информированности изучаемой области – средний балл равен 3,96 и более низкой степени аргументации – 3,82 балла.

Таблица 4 – Сводная группировка экспертов по оценочным баллам

Интервалы оценок в баллах	от 3,0 до 3,5	от 3,6 до 4,0	от 4,1 и выше	Всего
Количество экспертов, чел.	4	9	4	17
Средняя оценка по совокупности, балл	3,49	3,73	4,32	3,89

Характер распределения самооценки компетентности экспертов по оцениваемым областям знаний по пятибалльной шкале показывает достаточную близость к закону нормального распределения и сосредоточение средних оценок к средней величине, что свидетельствует о достаточно высокой компетентности экспертов и высоком качестве экспертизы. Приемлемая компетентность экспертов дает основание с достаточной степенью достоверности установить целесообразность включения частных показателей в обобщающие и их значимость на основании экспертизы.

Результаты экспертного оценивания показали весьма согласованные мнения по целесообразности включения предложенных частных показателей эффективности применения ИКТ – оценка превысила почти по всем показателям двухуровневую отметку и находится в переделах от 2 до 2,65 балла. При этом коэффициент согласованности мнений экспертов не превысил 20% уровень, приемлемый для обеспечения достоверности экспертизы. Такие же весьма согласованные мнения показали эксперты относительно значимости частных показателей эффективности в разрезе обобщающих показателей и обобщающих в составе интегральных показателей применения ИКТ – коэффициенты вариации мнений экспертов не превысил 20% уровень, приемлемый для обеспечения достоверности экспертизы.

Сводные результаты экспертной интегральной оценки эффективности применения ИКТ в инфокоммуникационных компаниях в 2016 и 2020 годах в баллах приведены в таблице 5. Результаты расчетов обобщающих показателей и интегрального коэффициента эффективности применения ИКТ в сфере инфокоммуникаций за пять лет в соответствии с интегрально-экспертным методом представлены в таблице 6.

Полученные результаты свидетельствуют о сложных процессах внедрения и применения ИКТ в производственной деятельности инфокоммуникационных компаний. Так в целом по интегральному коэффициенту эффективности в 2016 году, равному 0,75, можно говорить о недостаточном уровне эффективности применения ИКТ вследствие превышения затратного интегрального показателя эффективности применения ИКТ над результативным как по экономической, так и социальной составляющим эффективности с учетом положительных и отрицательных эффектов и последствий.

В то же время экспертные оценки эффективности применения ИКТ студентов показывают, что в результате динамичного развития инфокоммуникаций и построения информационного общества эффективность

применения ИКТ увеличивается к 2020 году в два раза и достигает величины 1,46 отн. ед. за счет роста положительного эффекта экономической и социальной эффективности и снижения отрицательного эффекта затратной составляющей эффективности применения ИКТ в России.

Таблица 5 – Сводные результаты экспертной оценки частных и обобщающих интегральных показателей эффективности применения ИКТ (по формуле средней арифметической) в сфере инфокоммуникаций (в баллах)

№	Частный показатель обобщающей оценки эффективности	Эффективность ИКТ в 2016г. (балл)	Эффективность ИКТ в 2020г. (балл)
1	***Обобщающий результативный показатель экономической эффективности (положительный эффект)***	***2,75***	***3,91***
1.1	Экономический рост за счет инновационного развития и внедрения ИКТ	2,82	3,88
1.2	Экономия трудовых ресурсов и рост производительности труда	3,00	3,71
1.3	Экономия материальных ресурсов	2,24	3,88
1.4	Увеличение доли информационных ресурсов в структуре ресурсов производства	2,76	4,18
1.5	Снижение технологических рисков	2,53	3,88
1.6	Рост оперативности управления производством	3,12	3,94
2	***Обобщающий результативный показатель социальной эффективности (положительный эффект)***	***2,29***	***4,13***
2.1	Рост интеллектуальности труда	2,76	4,35
2.2	Повышение мобильности трудовых ресурсов	2,53	4,06
2.3	Возможность производства и покупки электронных услуг	2,65	4,18
2.4	Увеличение доли свободного времени	2,53	4,06
2.5	Автоматизация и роботизация производства	2,24	4,18
2.6	Автоматизация и роботизация жилья	1,06	3,94
3	***Обобщающий затратный показатель экономической эффективности (отрицательный эффект)***	***3,80***	***2,85***
3.1	Затраты на развитие инфраструктуры инфокоммуникаций	4,06	2,5
3.2	Затраты на информационное обучение	3,41	1,5
3.3	Затраты на информационную безопасность	2,71	5,0
3.4	Риски (информационные, кибернетические)	4,00	4,7
3.5	Региональные диспропорции в доступе к Интернет	4,06	1,7
3.6	Затраты на борьбу с кибертерроризмом	3,59	
4	***Обобщающий затратный показатель социальной эффективности (отрицательный эффект)***	***3,93***	***2,41***
4.1	Виртуализация ценностей, этики, морали	2,24	4,0
4.2	Ухудшение физического здоровья	2,53	3,5
4.3	Ухудшение психологического здоровья	2,53	3,9
4.4	Формирование клипового мышления	3,18	4,7
4.5	Электронное неравенство	3,35	1,5
4.6	Неспособность людей противостоять информационному мошенничеству	3,76	2,7
Интегральный коэффициент эффективности применения ИКТ		***0,66***	***1,53***

Таблица 6 – Динамика обобщающих и интегральных показателей эффективности применения ИКТ в сфере инфокоммуникаций за пять лет в соответствии (по формуле средней арифметической взвешенной) в соответствии с интегрально-экспертным методом

Наименование показателей	Эффективность ИКТ в (в баллах)		Темп изменения за 2016-2020гг., %
	2016г.	2020г.	
1. Обобщающий результативный показатель экономической эффективности (положительный эффект)	2,8	3,9	140,0
2. Обобщающий результативный показатель социальной эффективности (положительный эффект)	2,3	4,1	179,0
Результативный интегральный показатель эффективности ИКТ	2,63	4,00	152,0
3. Обобщающий затратный показатель экономической эффективности (отрицательный эффект)	3,8	2,9	77,0
4. Обобщающий затратный показатель социальной эффективности (отрицательный эффект)	2,9	2,4	83,0
Затратный интегральный показатель эффективности ИКТ	3,51	2,37	68,0
Коэффициент интегральной эффективности применения ИКТ	0,75	1,46	1,95

Модель интегральной оценки эффективности инновационных решений с учетом синергетического эффекта в сфере спутниковой связи

Методика комплексной оценки эффективности инноваций, основанная на экспертно-квалиметрическом подходе с количественным выражением результатов экспертного оценивания, не только дает возможность повысить достоверность результатов выбора эффективных инноваций, но и обосновать управленческие решения в сфере инновационного развития инфокоммуникаций на основе построения интегральных показателей.

Зависимость стратегии развития спутниковой связи на основе новых технологий, в том числе с использованием новых диапазонов частот и высокоэллиптических орбит, от множества факторов социально-экономического, технического и политического характера, а также присутствующие в рыночной среде неопределенность и инвариантность поведения потребителей в сфере услуг спутниковой связи диктуют необходимость применения интегральных оценок эффективности инновационных проектов, формирования облика систем спутниковой связи [41].

В условиях существования и конкуренции различных видов проводной и беспроводной связи, множества влияющих на эффективность функционирования систем спутниковой связи факторов социально-экономического, технического и политического характера, методическим подходом к построению методики интегральной оценки эффективности

инновационных решений является раскрытие ее сущности как результата многофакторного процесса. На наш взгляд, под эффективностью инновационных проектов или решений в области систем спутниковой связи, различающихся использованием космических аппаратов на различных орбитах с разным обликом построения, следует понимать результативность качественного изменения потенциала производства услуг связи на основе применения уникальных технологий, систем и оборудования спутниковой связи.

Применение уникальных технологий, систем и оборудования спутниковой связи способствует переходу к более совершенному состоянию производства и потребления инфокоммуникационных услуг по организационно-экономическим и рыночно-технологическим параметрам. Эффект от применения различных систем и обликов построения спутниковой связи с использованием космических аппаратов (КА) имеет синергетический характер и определяется совместным результатом реализации рыночного, технического, социально-экономического потенциала данных систем.

Для определения понятия потенциала реализации инновационных решений (в частности, применения различных систем и обликов построения спутниковой связи с использованием КА на высокоэллиптических орбитах) можно исходить из следующих научных и логических предпосылок. С одной стороны, потенциал характеризуется степенью возможного проявления какого-либо явления, действия, функции, с другой стороны – потенциал проявляется в возможности достижения более высоких показателей, чем уже достигнуты. Вторая трактовка понятия потенциала подходит для решения поставленной задачи выбора наиболее эффективного варианта формирования облика системы спутниковой связи с точки зрения реализации их потенциальных возможностей по повышению качества и прогрессивности инфокоммуникационных услуг и обеспечению сбалансированности уровня их потребления по регионам страны, включая труднодоступные регионы и Арктическую зону [42].

Эффективность различных систем и обликов построения спутниковой связи в России и за рубежом определяются целым рядом факторов, которые можно разделить на несколько групп. В каждой группе факторов присутствуют как объективные, так и субъективные факторы и условия эффективного функционирования систем спутниковой связи. Объективные факторы охватывают внешнюю среду деятельности операторов спутниковой связи, субъективные – внутреннюю среду рыночного пространства.

Комплексная система интегральной оценки эффективности построения систем спутниковой связи (ССС) включает три блока обобщающих оценок, базирующихся на системе частных показателей (рис. 10). В состав комплексной системы интегральной оценки эффективности построения ССС входят: интегральный индекс эффективности построения систем спутниковой связи ($I_{ИНТ}$), обобщающие индексы рыночного потенциала ($I_{РЫН}$), технического потенциала ($I_{ТЕХН}$), социально-экономического потенциала ($I_{ЭКОН}$), рассчитываемые по совокупности наиболее значимых частных показателей [32].

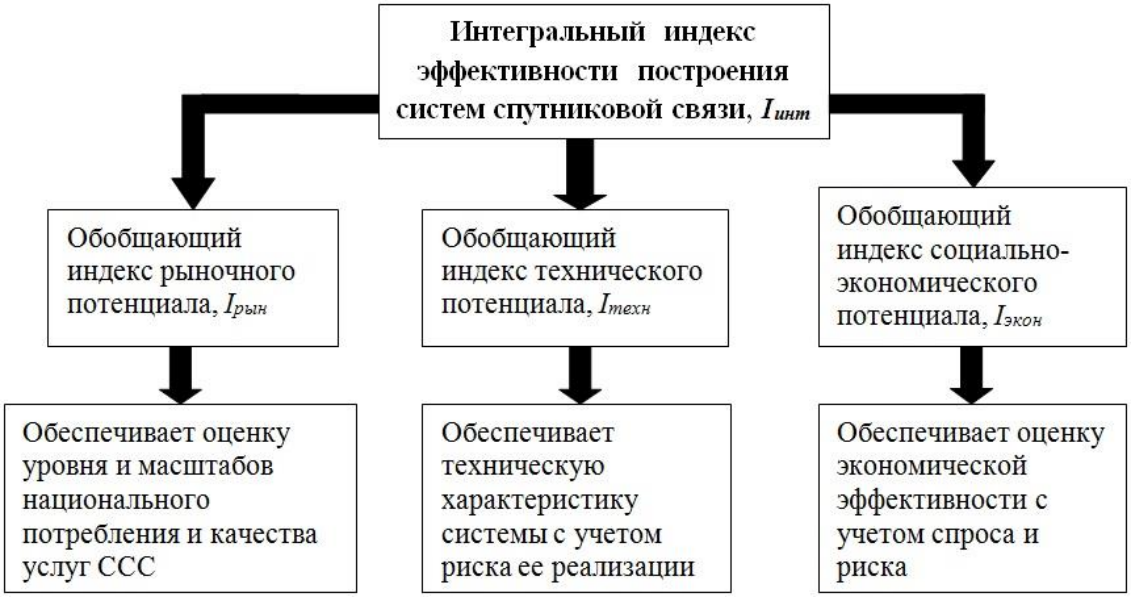


Рис. 10. Комплексная система интегральной оценки эффективности построения систем спутниковой связи

Для измерения обобщающего индекса рыночного потенциала можно использовать показатели, характеризующие рыночный потенциал услуг фиксированной и подвижной спутниковой связи, непосредственного звукового и мультимедиа вещания на территории Российской Федерации с выделением зон основных транспортных магистралей и густонаселенных районов РФ, Акватории Северного ледовитого океана и морей, Арктической зоны РФ, а также рыночный потенциал высокоскоростных мультимедийных услуг в 9-ти возможных перенацеливаемых зонах на территории РФ, по степени востребованности конкретной услуги в указанной зоне обслуживания.

Для измерения обобщающего индекса технического потенциала целесообразно применять показатели, характеризующие, в первую очередь, инновационность варианта системы спутниковой связи, космического сегмента и наземной инфраструктуры связи и управления космическими аппаратами, создаваемого абонентского оборудования для конкретного варианта по степени новизны применяемых решений и технологий, а именно: технических решений применяемых в бортовых радиотехнических комплексах (БРТК), для создания центральных стаций спутниковой связи (применяемых для загрузки и управления КА), оборудования каналообразования и управления услугами, для создания абонентских терминалов с заданными параметрами.

Для оценки технического потенциала важно также учитывать риски реализуемости системы в целом, ее космического сегмента, наземной инфраструктуры связи и управления КА, создаваемого абонентского оборудования для конкретного варианта по степени технических и технологических рисков создания всех составных частей системы, создания БРТК, наземной инфраструктуры связи и управления КА, создания абонентских терминалов с заданными параметрами приемлемой (доступной для массового потребителя) стоимости, а также риска возникновения нештатных ситуаций на

орбите по уровню вероятности выхода из строя элементов БРТК, критически влияющих на предоставление услуг связи. Немаловажное значение для измерения технического потенциала имеет возможность использования существующих технологий, решений для создания космического и наземного сегментов конкретных вариантов ССС, которую можно оценить по показателю степени использования существующих отработанных технологий и решений для БРТК, отработанных технологий и оборудования для наземной инфраструктуры связи.

Оценка обобщающего индекса социально-экономического потенциала может производиться с помощью общеизвестных показателей удельной общей стоимости системы ССС, удельной себестоимости услуг оказания услуг (на одного пользователя), обеспечения потребностей в услугах связи госзаказчиков (спецпотребителей) на территории РФ и в Арктической зоне, уровня внешних (мировых) и внутренних политических и социально-экономических рисков. На величину внешних политических и социально-экономических рисков оказывают влияние мировые финансовые кризисы, введение экономических санкций, развязывание военных действий, стихийные бедствия глобального масштаба. В то же время снижение темпов экономического роста, ВВП, экспорта национальных продуктов, инвестиций в развитие общественного производства, трудовых ресурсов, уровня социального и материального благосостояния, стихийные бедствия национального масштаба – это важнейшие факторы внутренних рисков, негативно влияющих на социально-экономические показатели внедрения и реализации рассматриваемых вариантов построения ССС.

В условиях активизации процессов информатизации и необходимости освоения новых источников природных ресурсов важное значение приобретают такие показатели как: степень влияния внедрения услуг ССС России на рост доступности услуг связи (Интернет) и информационных ресурсов и снижение цифрового разрыва населения на территории РФ и в Арктической зоне (измеряемой степенью доступности услуг для населения), степень влияния внедрения услуг систем спутниковой связи России на освоение природных ресурсов, развитие производства и рост ВВП РФ (измеряемой увеличением темпов прироста объемов добычи природных ресурсов, производства, ВВП РФ за счет синергетического эффекта от создания систем спутниковой связи). Развитие рыночных инструментов диктует необходимость применения показателя «уровень интеграции бизнеса в сфере создания ССС Российской Федерации», оцениваемого степенью (процентом) участия иностранных компаний в совместном производстве систем и компонентов систем спутниковой связи, передачей передовых технологий.

Для получения комплексной оценки эффективности различных вариантов построения систем спутниковой связи и принятия адекватных управленческих решений на государственном уровне необходима разработка организационно-методического инструментария обоснования выбора наиболее эффективного варианта построения систем спутниковой связи с учетом комплекса факторов и синергетического эффекта. При этом следует учесть, что большинство

сравниваемых показателей вариантов построения систем спутниковой связи не имеют количественного выражения или отсутствуют в виде статистических или выборочных данных.

Рассмотренные нами методы исчисления комплексных показателей и применение технологии экспертного опроса эффективности вариантов построения ССС с оценкой целесообразности введения в модель частных показателей и значимости частных и обобщающих показателей дают основание для формирования модели интегрального показателя (индекса) эффективности построения ССС на основе средних арифметической или геометрической, а также метода расстояний как по простой, так и взвешенной формул [32].

Если используются результаты оценки экспертами эффективности варианта построения системы спутниковой связи типа в баллах, то можно исчислять интегральный и обобщающие показатели эффективности в баллах на основе средней арифметической простой и взвешенной. Если применить прием расчета обобщающих и частных показателей в относительных единицах (например, относительно средней по совокупности частных показателей), то рассчитывается интегральный индекс эффективности построения ССС на основе средней геометрической взвешенной. Метод расстояний может применяться как при расчете интегрального и обобщающих показателей эффективности (в абсолютном выражении), так и интегрального и обобщающих индексов эффективности (в относительном выражении).

Интегральный показатель и обобщающие показатели рыночного, технического и социально-экономического потенциалов эффективности формирования облика ССС на основе баллов в абсолютном измерении рассчитываются по формуле средней арифметической простой и взвешенной:

$$П_{ИНТ} = (П_{РЫН} + П_{ТЕХН} + П_{ЭКОН})/3;$$
$$П_{ИНТ} = (П_{РЫН} \cdot 1/3 + П_{ТЕХН} \cdot 1/3 + П_{ЭКОН} \cdot 1/3);$$
$$П_{ОБОБ} = \frac{\sum_{j=1}^{m} (П_j \cdot d_j)}{m}, \quad (7)$$

где $П_{ИНТ}$ - интегральный показатель эффективности построения ССС; $П_j$ - j–тый частный показатель в разрезе обобщающих показателей; d_j - значимость j–того частного показателя; m - количество j–тых частных показателей (по рыночному потенциалу частных показателей 13; по техническому потенциалу – 11; по социально-экономическому - 10); $П_{РЫН}$, $П_{ТЕХН}$, $П_{ЭКОН}$ - обобщающие показатели рыночного, технического, социально-экономического потенциала.

Для исчисления компонентов модели интегральной оценки эффективности вариантов формирования облика ССС можно произвести расчет обобщающих индексов рыночного, технического и социально-экономического потенциалов по формуле средней геометрической взвешенной относительных величин частных показателей (относительно индивидуальных средних в разрезе обобщающих показателей или общей средней по обобщающему показателю).

Модель интегрального индекса эффективности построения ССС на основе средней геометрической взвешенной имеет вид:

$$I_{ИНТ} = \sqrt[n]{П(I_i \cdot d_i)},\ I_{ОБОБ} = \sqrt[m]{П(I_j \cdot d_j)}, \quad (8)$$

где $I_{ИНТ}$ - интегральный индекс эффективности построения ССС; I_i - i–тый обобщающий индекс; d_i - значимость i–того обобщающего индекса; n - количество обобщающих индексов; $I_{ОБОБ}$ ($I_{РЫН}$, $I_{ТЕХН}$, $I_{ЭКОН}$) - обобщающие индексы рыночного, технического, социально-экономического потенциала; I_j - j–тый частный индекс (относительно к индивидуальной или общей средней в разрезе конкретных обобщающих показателей) (отн. ед.); m - количество j–тых частных индексов.

Модели интегрального показателя и индекса эффективности построения ССС по методу расстояний строятся с помощью трех обобщающих показателей эффективности построения систем спутниковой связи на основе абсолютных и относительных величин частных и соответственно обобщающих показателей и имеют вид:

$$П_{ИНТ} = \sqrt{П^2_{РЫН} \cdot 1/3 + П^2_{ТЕХН} \cdot 1/3 + П^2_{ЭКОН} \cdot 1/3},$$
$$I_{ИНТ} = \sqrt{I^2_{РЫН} \cdot 1/3 + I^2_{ТЕХН} \cdot 1/3 + I^2_{ЭКОН} \cdot 1/3},$$
$$П_{ОБОБ} = \sqrt{\sum_{j=1}^{m} П_j^2 \cdot d_j},\ \ I_{ОБОБ} = \sqrt{\sum_{j=1}^{m} I_j^2 \cdot d_j} \quad (9)$$

Методика обоснования выбора оптимального варианта формирования облика системы спутниковой связи на основе интегрального подхода к измерению эффективности построения ССС с учетом совокупности внешнеэкономических и внутренних условий и факторов социально-экономического развития Российской Федерации посредством экспертной оценки параметров эффективности балльным методом представлена на рис. 11.

Методический аппарат обоснования факторов и параметров модели интегральной оценки эффективности построения систем спутниковой связи реализуется на основе экспертных данных о целесообразности включения тех или иных частных показателей в обобщающие и интегральный показатели и их значимости для интегральной оценки, статистической обработки информации, полученной методом экспертного опроса, анализа вариации показателей и тесноты связи между ними для выбора наиболее существенных параметров и формирования обобщающих показателей – компонентов интегральной модели, проведения аналитических работ по оценке достоверности и интерпретации результатов моделирования и оценки эффективности систем спутниковой связи.

Для обоснования наиболее важных показателей интегральной оценки эффективности построения систем спутниковой связи, а также оценки сопоставительной значимости частных показателей в обобщающих показателях по конкретным направлениям эффективности построения систем спутниковой связи (рыночная, техническая, социально-экономическая) используется метод экспертных оценок (метод «Дельфи»), позволяющий обобщать мнения отдельных экспертов в согласованное групповое мнение [26, 28, 34].

Рис. 11. Методика обоснования факторов и параметров модели интегральной оценки эффективности построения систем спутниковой связи

Достижение целей интегральной оценки эффективности вариантов формирования облика системы спутниковой связи на основе метода экспертных оценок обеспечивается последовательным решением пяти задач:

- первой задачей эксперта является самооценка компетентности посредством оценки в баллах степени информированности и аргументации решения проблемы;
- второй задачей является ознакомление с краткой характеристикой предлагаемых вариантов формирования облика системы спутниковой связи с использованием космических аппаратов, включая сравнение зон обслуживания предлагаемыми вариантами связи;
- третья задача эксперта состоит в изучении предложенной системы показателей интегральной оценки эффективности построения ССС и выражение собственного мнения о целесообразности включения конкретных показателей в модель интегральной оценки эффективности формирования облика ССС в баллах по десятибалльной шкале и его значимости (весе) в процентах. Эксперт имеет право поставить низкую оценку какому-либо показателю и предложить один или несколько других показателей, более важных, по

его мнению, для комплексной оценки эффективности спутниковой группировки, чем предложенные;
- четвертая задача эксперта состоит в установлении значимости частных показателей в разрезе обобщающих показателей модели интегральной оценки эффективности построения ССС (в %);
- пятая задача экспертов состоит в непосредственной оценке эффективности двух вариантов построения ССС путем установления баллов по десятибалльной шкале.

В состав экспертной группы по достижению поставленных целей должны входить высококвалифицированные специалисты с перспективным и стратегическим типом мышления, способные предвидеть будущее развитие систем и оборудования спутниковой связи и системно оценивать результаты развития спутниковой связи страны с учетом национальных особенностей социально-экономического развития России, внешних и внутренних рисков и конъюнктуры национального и международного рынка услуг спутниковой связи.

Интегральная оценка результатов экспертизы эффективности вариантов построения систем спутниковой связи

Сводные результаты самооценки экспертов по обоснованию состава, значимости показателей и оценке эффективности вариантов формирования облика системы спутниковой связи представлены на рис. 12. Характер распределения самооценки компетентности экспертов по оцениваемым областям знаний по пятибалльной шкале показывает достаточную близость к закону нормального распределения и сосредоточение средних оценок к средней величине, что свидетельствует о достаточно высокой компетентности экспертов и высоком качестве экспертизы.

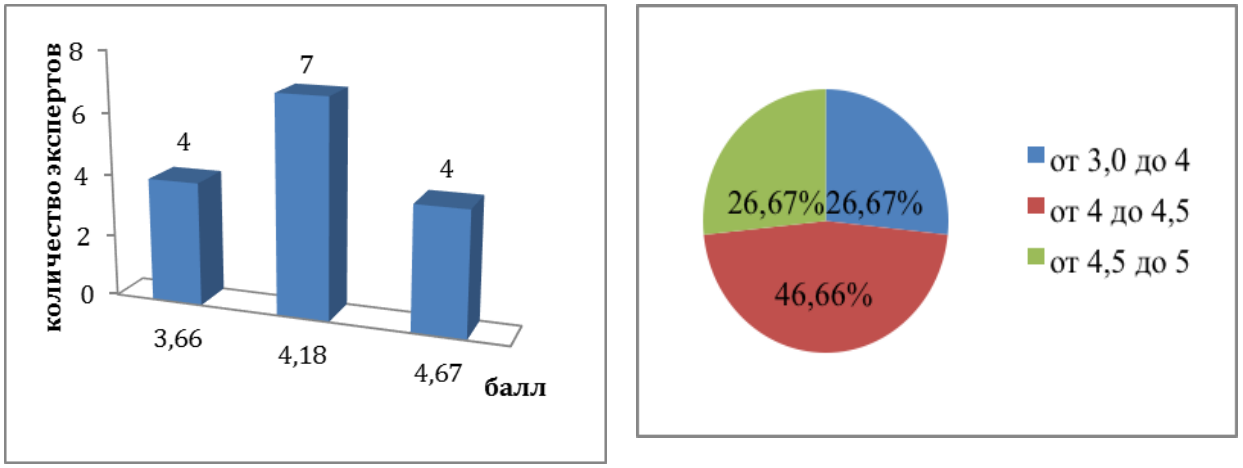


Рис. 12. Распределение самооценки компетентности экспертов по обоснованию состава, значимости показателей и оценке эффективности вариантов формирования облика системы спутниковой связи

Проведенная экспертиза целесообразности включения частных показателей в три обобщающих показателя и в модель интегральной оценки

эффективности построения ССС показала, что все эксперты признали состав предложенных частных показателей как совокупность значимых параметров модели (рис. 13). Коэффициенты согласованности мнений экспертов по каждому из этих показателей находятся в пределах 20% (от 11,0% до 19,22%), что является достаточно удовлетворительным для социально-экономических исследований.

Представленная на рис. 13 характеристика экспертных оценок целесообразности включения частных показателей в обобщающие показатели эффективности построения ССС показывает превышение оценок по всем видам обобщающих показателей уровня в 7 баллов: большая половина частных показателей, входящих в обобщающие показатели, превышает 7,5 баллов. Особенно высокие баллы целесообразности предложенных показателей отданы частным показателям рыночного потенциала. Для частных показателей обобщающих показателей «Технический потенциал» и «Социально-экономический потенциал» характерна такая же картина экспертных оценок с доминированием высоких баллов – для 7 показателей экспертами выставлены баллы, превышающие 8 баллов.

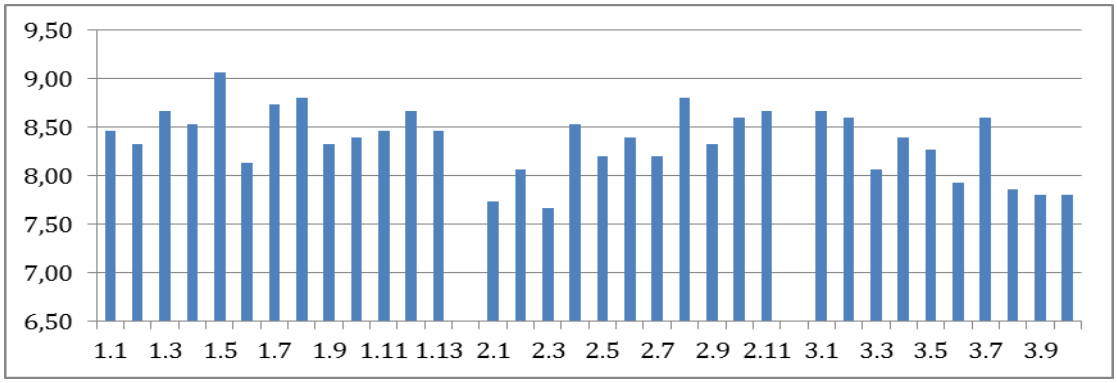


Рис. 13. Характеристика экспертных оценок целесообразности включения частных показателей в обобщающие показатели эффективности построения ССС: рыночный потенциал (с 1.1 до 1.13 показатель), технический потенциал (с 2.1 до 2.11 показатель), социально-экономический потенциал (с 3.1 до 3.10 показатель)

Сводные результаты экспертизы о значимости частных показателей в разрезе обобщающих показателей интегральной оценки эффективности показали достаточно согласованные оценки значимости всех показателей эффективности формирования облика спутниковой связи (рис. 14).

По экспертным оценкам значимости частных показателей, входящих в состав обобщающих показателей, можно также получить весьма убедительные выводы – все показатели признаны экспертами значимыми с достаточно высокими балльными оценками, находящимися в пределах 6 и более баллов. Согласованность мнений экспертов по оценке веса частных показателей в обобщающем позволяет использовать их в качестве типичных величин значимости частных показателей при построении модели интегральной оценки эффективности формирования облика спутниковой связи.

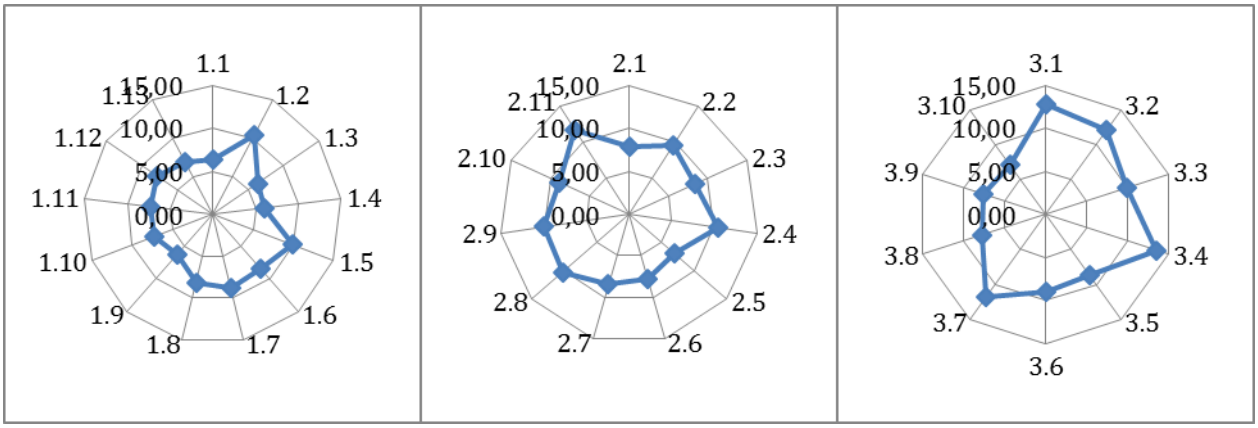


Рис. 14. Результаты экспертизы о значимости частных показателей в разрезе обобщающих показателей модели интегральной оценки эффективности построения систем спутниковой связи

Объемный график результатов экспертной интегральной оценки эффективности вариантов формирования облика ССС по частным показателям в разрезе обобщающих показателей позволяет наглядно сопоставить эффективность вариантов построения ССС по различным потенциалам (рис. 15). Так из графика видно, что второй вариант по многим показателям технического и социально-экономического потенциалов имеет определенные преимущества, что диктует необходимость обоснования модели интегральной оценки эффективности построения системы спутниковой связи.

Для подтверждения научной обоснованности применения разных формул модели интегральной оценки эффективности формирования облика ССС по разным формулам нами произведены различные варианты расчетов, в первую очередь, на основе применения средней арифметической (простой и взвешенной) по абсолютным показателям в баллах, средней геометрической - по относительным величинам в двух ракурсах – относительно среднего балла по каждому эксперту и по общей средней по всей совокупности экспертов.

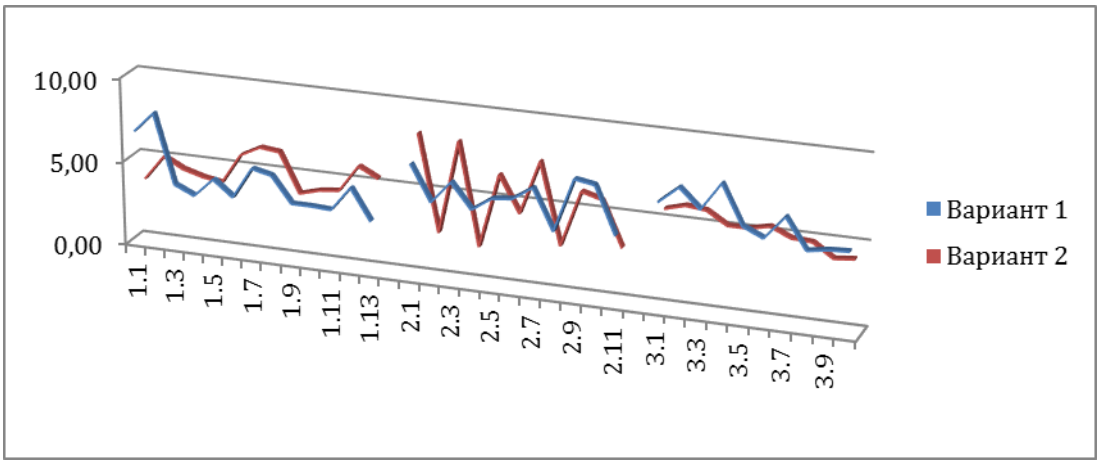


Рис. 15. Сопоставление результатов экспертной интегральной оценки эффективности вариантов формирования облика систем спутниковой связи по частным показателям в баллах в разрезе обобщающих показателей

Сводные результаты экспертной интегральной оценки эффективности вариантов формирования облика ССС по абсолютным показателям по простой и взвешенной (с учетом значимости показателей) средней арифметической показывают более высокую эффективность первого варианта формирования облика ССС на основе космических аппаратов среднего класса по сравнению с КА тяжелого класса по двум обобщающим показателям технического и социально-экономического потенциалов.

В то же время по обобщающему показателю рыночного потенциала более высокую эффективность имеет второй вариант построения системы спутниковой связи, имеющий более широкую возможность охвата территории инновационными услугами мультимедийного характера. Из приведенной столбиковой диаграммы следует, что это произошло вследствие более высоких значений рыночного потенциала предоставления услуг фиксированной спутниковой связи (ФСС) в первом варианте облика спутниковой системы, более высокой эффективности по удельным величинам стоимости системы и себестоимости оказания услуг, обеспечения потребностей услуг госзаказчиков на территории страны и в Арктической зоне при более высоких значениях рисков реализуемости проекта во втором варианте.

Хотя результаты оценки эффективности вариантов формирования облика ССС по формуле средней арифметической взвешенной показали аналогичные результаты, но разрыв в оценках эффективности вариантов по модели средневзвешенной арифметической увеличился по техническому и социально-экономическому потенциалам вследствие более высоких величин значимости показателей рисков технического потенциала: реализуемости системы, ее космического сегмента, абонентского оборудования и возникновения нештатных ситуаций на орбите, и показателям социально-экономического потенциала: удельной стоимости системы, себестоимости оказания услуг, обеспечения потребностей в услугах связи госзаказчиков (спецпотребителей) в Арктической зоне и влияния внедрения услуг спутниковой связи России на рост доступности услуг связи (Интернет) и информационных ресурсов и снижение цифрового разрыва населения в Арктической зоне.

Применение разных средних для измерения относительных частных показателей эффективности позволяет в первом случае учесть вариацию индивидуальных мнений экспертов, во втором – общую вариацию частных показателей в разрезе обобщающих показателей, тем самым индивидуализировать или обобщить оценки экспертов. Результаты интегральной оценки эффективности вариантов формирования облика систем спутниковой связи по модели средней геометрической на основе относительных значений к индивидуальной и общей средней оценке эксперта показывают аналогичные результаты.

Анализ вариации экспертных оценок по частным показателям в разрезе обобщающих показателей и соответственно интегральной оценки эффективности построения ССС показал, что коэффициенты согласованности мнений экспертов по оценкам частных показателей находятся в пределах 15%

(от 10,7% до 14,86%), что является весьма удовлетворительным для социально-экономических исследований.

Сводные результаты оценки эффективности вариантов построения ССС по разным формулам и обобщающим компонентам модели интегральной оценки представлены в таблице 8.

Таблица 8 – Сопоставление экспертных оценок эффективности вариантов (№ 1 и № 2) построения систем спутниковой связи по разным формулам модели интегральной оценки

Формула модели интегральной оценки	Рыночный потенциал		Технический потенциал		Социально-экономический потенциал		Коэффициент эффективности	
	№1	№2	№1	№2	№1	№2	№1	№2
Средняя арифметическая простая	4,57	4,79	5,61	5,12	5,96	5,03	***5,38***	***4,98***
Средняя арифметическая взвешенная	4,70	4,855	5,528	4,906	6,178	5,122	***5,47***	***4,96***
Средняя геометрическая по индивидуальной средней экспертов	0,9575	0,980	0,9785	0,8866	0,9858	0,9935	***0,9739***	***0,9534***
Средняя геометрическая по общей средней	0,9592	0,982	0,9802	0,8949	0,9846	0,9916	***0,9747***	***0,9562***
Метод расстояний по абсолютным частным показателям	4,93	4,94	5,64	5,39	6,27	5,16	***5,64***	***5,166***
Метод расстояний по относительным частным показателям	1,08	1,03	1,01	1,05	1,05	1,02	***1,046***	***1,036***

В результате проведенной апробации разных формул модели интегральной оценки эффективности построения систем спутниковой связи получены результаты свидетельствующие о возможности применения разных формул методологии комплексного экономического анализа, дающих одинаковые общие результаты об эффективности варианта формирования облика ССС с использованием космических аппаратов среднего класса.

В то же время применение интегрального подхода к моделированию оценки эффективности с помощью обобщающих показателей позволяет получить выводы об эффективности второго варианта формирования облика систем спутниковой связи с использованием космических аппаратов тяжелого класса по рыночному потенциалу. Данный методический подход к параметрической оценке эффективности позволяет говорить о том, что второй вариант построения системы спутниковой связи на базе КА тяжелого класса также эффективен, но для ее обеспечения необходимо решить инвестиционные и инновационные вопросы [32].

Таким образом, на основе выявления характера влияния факторов на различные варианты построения ССС и проявления синергетического эффекта их функционирования сформирована система показателей и модель интегральной оценки эффективности вариантов построения систем спутниковой связи, получены сводные и частные результаты ее оценки с помощью процедуры экспертного оценивания состава, значимости частных показателей интегральной модели и непосредственной оценки эффективности. Оценка достоверности выбора эффективных вариантов построения систем спутниковой связи осуществлена на основе коэффициента согласованности мнений экспертов и апробации различных подходов к построению интегрального показателя эффективности.

Заключение

Действующие методы оценки эффективности инновационных проектов, построенные на стоимостном измерении ограниченного круга показателей, в условиях усложнения экономических отношений и множественности проявлений эффектов не могут решить все стоящие перед стратегическим менеджментом задачи обоснованного выбора наиболее эффективных управленческих решений, вариантов развития, инноваций и применения новых технологий, а также учесть синергетический эффект и влияние факторов.

Неполнота информации на ранних стадиях жизненного цикла новшеств, неопределенность последствий их реализации на рынке, невозможность отразить в стоимостных показателях всех проявлений эффектов диктуют необходимость системного решения проблемы количественной оценки эффективности на основе качественных методов и интегральных способов формирования комплексных показателей. Система показателей эффективности инновационных решений должна не только определять интегральный уровень состояния и потенциала развития любого объекта оценки эффективности, но и возможность ранжирования и выбора наиболее эффективных объектов из множества альтернатив.

Инструментом реализации данной проблемы является экспертно-квалиметрический метод комплексной оценки эффективности на основе применения достижений науки и практики в области экспертных технологий, методов квалиметрии и комплексного оценивания. Количественный учет множества влияющих факторов, частных показателей эффективности и выбор наиболее эффективных вариантов из множества альтернатив позволяет перевести систему инновационного менеджмента на более высокий уровень научного обоснования принятия решений с учетом множества факторов и специфических условий деятельности хозяйствующих субъектов.

Цель разработки экспертно-квалиметрического подхода первоначально состояла в формировании средств и методов обоснования выбора наиболее эффективных инноваций из множества альтернатив на первых этапах жизненного цикла, когда отсутствует количественная информация о результатах и последствиях внедрения инноваций. В основе этого метода лежит рассмотрение эффективности как совокупности свойств, отражающих

отдельные проявления эффектов и барьеров внедрения инноваций, которые оценивают эксперты в количественной форме (в баллах), и комплексная форма выражения эффективности, уровень которой служит критерием выбора наиболее эффективных инноваций. Коэффициент эффективности инноваций позволяет не только четко в количественной форме оценить эффективность, но и ранжировать инновации.

Для применения экспертно-квалиметрического метода в различных областях инновационного менеджмента авторами дано методическое обоснование параметров модели комплексной оценки, их значимости, шкал измерения и процедуры экспертного оценивания эффективности инноваций произведено на основе аналитического материала о деятельности операторов связи и результатов экспертных оценок группы специалистов.

Применение экспертно-квалиметрического метода к оценке эффективности применения ИКТ с учетом эволюции параметров развития инфокоммуникаций во взаимосвязи с формированием информационного общества и характера проявления как положительного, так и отрицательного эффектов в экономической и социальной жизни позволило создать адекватную комплексную системы показателей эффективности ИКТ.

Комплексная система оценки экономической и социальной эффективности ИКТ имеет иерархическую систему и включает два блока интегральных оценок, отражающих положительные эффекты и отрицательные последствия применения ИКТ, базирующихся на системе обобщающих и частных показателей экономической и социальной эффективности. Апробация предложенной системы показателей позволила весьма достоверно оценить фактическую эффективность применения ИКТ в инфокоммуникационных компаниях, выявить узкие места и направления развития инфокоммуникаций и показать возможный уровень эффективности ИКТ через пять лет.

Экспертно-квалиметрический метод с количественным выражением результатов экспертного оценивания не только дает возможность повысить достоверность результатов выбора эффективных инноваций, но и обосновать управленческие решения по инновационному развитию, выбору вариантов построения систем, сетей и технологий на основе построения интегральных показателей.

Интегральный показатель эффективности представляет собой иерархическую систему обобщающих и частных показателей, отражающих различные проявления эффектов или потенциала развития, целесообразность и значимость которых устанавливается экспертами. Модели интегрального и обобщающих показателей эффективности инновационных решений основываются на известных методах построения комплексных оценок по средним величинам (арифметической простой и взвешенной, геометрической взвешенной) и методу расстояний. Апробация интегрального метода оценки эффективности построения двух вариантов систем спутниковой связи позволила обоснованно выбрать наиболее эффективный вариант с учетом синергетического эффекта и множества факторов и условий его реализации.

Литература

1. Кузовкова Т. А. Оценка роли инфокоммуникаций в национальной экономике и выявление закономерностей ее развития // Системы управления, связи и безопасности. 2015. № 4. С. 26-68.

2. Кузовкова Т. А., Тимошенко Л.С. Анализ и прогнозирование развития инфокоммуникаций. – М.: Горячая линия – Телеком, 2016. – 174 с.

3. Друкер П. Ф. Задачи менеджмента в XXI веке / Пер. с англ. – М.: Издат. дом «Вильямс», 2003. – 272 с.

4. Ламбен Жан Жак. Менеджмент, ориентированный на рынок / Пер. с англ. под ред. В.Б. Колчанова. – СПб.: Питер, 2004. – 800 с.

5. Фомичев А. Н. Стратегический менеджмент: Учебник для вузов. – М.: Издательско-торговая корпорация “Дашков и К”, 2011. – 468 с.

6. Друкер П. Ф. Бизнес и инновации. – М.: Вильямс, 2007. – 173 с.

7. Медынский В. Г. Инновационный менеджмент – М.: ИНФРА-М, 2007. – 458 с.

8. Инновационный менеджмент: Учебник / Под ред. В. А. Швандара, В. Я. Горфинкеля. – М.: Вузовский учебник, 2006. – 382 с.

9. Стратегический менеджмент / Под ред. А. Н. Петрова. – СПб.: Питер, 2005. – 496 с.

10. Голышко А. В., Степанов С. Н., Тихвинский В. О., Терентьев С. В. «Третий глаз» инновационного менеджера // Вестник связи. 2007. № 6. С. 54-65.

11. Кузовков Д. В. Экспертно-квалиметрическая оценка эффективности инноваций. – Саарбрюккен, Германия: LAMBERT Academic Publishing, 2015. – 136 с.

12. Богатин Ю. В., Швандар В. А. Оценка эффективности бизнеса и инвестиций: Учебное пособие. – М.: Финансы, ЮНИТИ-ДАНА, 1999. – 254 с.

13. Виленский П. Л., Лившиц В. Н., Смоляк С. А. Оценка эффективности инвестиционных проектов. Теория и практика. – М.: Дело, 2001. – 366 с.

14. Инновационный менеджмент / Под ред. Ильенковой С. Д. – М.: ЮНИТИ-ДАНА, 2007. – 343 с.

15. Косов В. В. Методические рекомендации по оценке эффективности инвестиционных проектов. – М.: Экономика, 2000. – 421 с.

16. Методические рекомендации по оценке эффективности инвестиционных проектов. – М.: Экономика, 2000. – 154 с.

17. Управление инновационными проектами: Учеб. Пособие / Под ред. В. Л. Попова. – М.: ИНФРА-М, 2007. – 336 с.

18. Фатхутдинов Р. А. Инновационный менеджмент: Учебник. – М.: СПб.: Питер, 2011. – 448 с.

19. Кузовков Д. В., Тураева Т. В. Экономическая оценка эффективности инвестиций и инноваций в инфокоммуникациях / Под ред. Т. А. Кузовковой . – М.: ООО «ИД Медиа Паблишер», 2013. – 250 с.

20. Большой экономический словарь / Под ред. А. Н. Азрилияна. – М.: Институт новой экономики, 2002. – 1280 с.

21. Аджемов А. С., Буйдинов Е. В., Кузовкова Т. А. Применение интегральной модели для оценки эффективности построения системы спутниковой связи // Электросвязь. 2016. № 4. С. 25-29.

22. Баканов М. И., Мельник М. В., Шеремет А. Д. Теория экономического анализа: Учебник. – М.: Финансы и статистика, 2005. – 536 с.

23. Вертакова Ю. В., Козьев И. А., Кузьбожев Э. Н. Управленческие решения: разработка и выбор: Учебное пособие / Под общ. ред. Э. Н. Кузьбожева. – М.: КНОРУС, 2005. – 352 с.

24. Шеремет А. Д. Теория экономического анализа: Учебник. – М.: ИНФРА-М, 2011. – 352 с.

25. Азгальдов Г. Г. Теория и практика оценки качества товаров: Основы квалиметрии. – М.: Экономика, 1982. – 256 с.

26. Волков В. И. Основы теории и практики экспертной деятельности. – М.: Академия менеджмента инноваций, 2002. – 196 с.

27. Кузовков Д. В. Применение экспертно-квалиметрического подхода к оценке эффективности инноваций и выбору поставщика оборудования в сфере инфокоммуникаций // Век качества. 2009. № 1. С. 30-33.

28. Литвак Б. Г. Экспертные технологии в управлении: Учебное пособие. – М.: Дело, 2004. – 400 с.

29. Мазур И. И., Шапиро В. Д. Управление качеством. – М.: Издательство «Омега – Л», 2008 – 399 с.

30. Фомин В. Н. Квалиметрия. Управление качеством. Сертификация: Учебное пособие. – М.: Ось-89, 2007. – 384 с.

31. Азгальдов Г. Г, Костин А. В., Садовов В. В. Квалиметрия: первоначальные сведения. Справочное пособие с примером для АНО «Агентство стратегических инициатив по продвижению новых проектов»: Учеб. Пособие. – М.: Высш. шк., 2011. – 143 с.

32. Аджемов А. С., Буйдинов Е. В., Кузовков Д. В. Применение экспертно-квалиметрическоо метода для обоснования выбора эффективных инноваций в спутниковой связи // Электросвязь. 2015. № 1. С. 27-30.

33. Тихвинский В. О., Кузовков Д. В. Экспертно-квалиметрический подход к обоснованию выбора инноваций и поставщиков оборудования в сфере инфокоммуникаций // Вестник РАЕН. 2009. №3. С. 58–64.

34. Малин А. С., Мухин В. Н. Исследование систем управления: Учебник для вузов. – М.: Изд. дом ГУ ВШЭ, 2005. – 399 с.

35. Кузовкова Т. А., Пронин А. М., Салютина Т. Ю., Тимошенко Л. С., Устинова Ю. С., Шаравова О. И. Статистика связи: Учебник для вузов. – М.: Радио и связь, 2003. – 624 с.

36. Государственная программа «Информационное общество (2011-2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 15 апреля 2014 года № 313.

37. Кузовкова Т. А., Женчур М. А., Кузовков А. Д. Методический аппарат комплексного прогнозирования развития инфокоммуникаций // Системы управления, связи и безопасности. 2016. № 1. С. 146-190.

38. Салютина Т. Ю., Кузовков А. Д. Комплексная оценка развития инфокоммуникаций и формирования информационого общества на основе интегрального и экспертного методов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону: ПЦ "Университет" СКФ МТУСИ. 2016. С. 478–484.

39. Индикаторы информационного общества: 2013: статистический сборник. – М.: НИИ «ВШЭ», 2013. – 328 с.

40. Карышев М. Ю. Специфика применения международной статистической методологии измерения информационного общества в России // Экономика, Статистика и Информатика. 2011. № 4. С. 89-92.

41. Стратегия развития ФГУП «Космическая связь» на 2011-2015 годы и на период до 2020 г. – М.: ГП КС, 2013. – 278 с.

42. Об утверждении государственной программы Российской Федерации «Социально-экономическое развитие Арктической зоны Российской Федерации на период до 2020 года». Постановление Правительства РФ от 21 апреля 2014 г. № 366.

References

1. Kuzovkova T. A. *Ocenka roli infokommunikacii v nacionalnoi ekonomike i viyavlenie zakonomernostej ee razvitiya* [Evaluation of the role of infocommunication in the national economy and the identification of regularities of its development]. *Systems of Control, Communication and Security*, 2015, no 4, pp. 26-68 (in Russian).

2. Kuzovkova T. A., Timoshenko L. S *Analiz i prognozirovanie razvitiia infokommunikacii* [Analysis and Forecast of Infocommunication Development]. Moscow, Goriachaia Liniia-Telekom Publ., 2016, 174 p. (in Russian).

3. Drucker P. F. *Management Challenges for the 21st Century*. New York, Harper Business publ., 1999. 207 p. (in Russian).

4. Lambin J. J. *Market-Driven management: Strategic and Operational Marketing*. London: Macmillan press, 2000. 737 p. (in Russian).

5. Fomichev A. N. *Strategicheskij menedzhment* [Strategic management]. Moscow, Izdatelsko-torgovaya korporaciya “Dashkov i Ko” Publ., 2011. 468 p. (in Russian).

6. Drucker P. F. *Innovation and Entrepreneurship Principles and Practices*. New York, HarperCollins publishers, 1985. 277 p. (in Russian).

7. Medinskij V. G. *Innovacionnij menedzhment* [Innovation management]. Moscow, INFRA-M Publ., 2007. 458 p. (in Russian).

8. Shvandar V. A., Gorfinkel V. Y. *Innovacionnij menedzhment* [Innovation management]. Moscow, Vuzovskij Uchebnik Publ., 2006. 382 p. (in Russian).

9. Petrov A. N. *Strategicheskij menedzhment* [Strategic management]. Saint-Petersburg, Piter Publ., 2005. 496 p. (in Russian).

10. Golishko A. V., Stepanova S. N., Tihvinskij V. O., Terentiev S. V. “Tretij glaz” innovacionnogo menedzhmenta [Innovation management’s “Third eye”]. *Vestnik svyazi*, 2007, vol. 6, pp. 54-65 (in Russian).

11. Kuzovkov D. V. *Expertno-kvalimetricheskaya ocenka effektivnosti innovacij* [Expert-qualimetric evaluation of the effectiveness of innovation]. Saarbrucken, Germany, LAMBERT Academic Publishing, 2015. 136 p. (in Russian).

12. Bogatin Y. V., Shvandar V. A. *Ocenka effectivnosti biznesa i investicij* [Efficiency evaluation of business and investment]. Moscow, "Finances" UNITI-DANA Publ., 1999. 254 p. (in Russian).

13. Vilenskij P. L., Livshic V. N., Smolyak S. A. *Ocenka effectivnosti investicionnih proektov. Teoriya i praktika* [Efficiency evaluation of investment projects. Theory and practices]. Moskow, Delo Publ., 2001. 366 p. (in Russian).

14. Ilienkova S. D. *Innovacionnij menedzhment* [Innovation management]. Moscow, UNITI-DANA, 2007. 343 p. (in Russian).

15. Kosov V. V. *Metodologicheskie rekomendacii po ocenke effektivnosti investicionnih proektov* [Methodological recommendations for efficiency evaluation of investment projects]. Moscow, Economics Publ., 2000. 421 p. (in Russian).

16. *Metodologicheskie rekomendacii po ocenke effektivnosti investicionnih proektov* [Methodological recommendations for efficiency evaluation of investment projects]. Moscow, Economics Publ., 2000. 154 p. (in Russian).

17. Popov V. L. *Upravlenie investicionnimi proektami* [Investment projects management]. Moscow, INFRA-M, 2007. 336 p. (in Russian).

18. Fathutdinov R. A. *Innovacionnij menedzment* [Innovation managemet]. Saint-Petersburg, Piter Publ., 2011. 448 p. (in Russian).

19. Kuzovkov D. V., Turaeva T. V., Kuzovkova T. A. *Economicheskaya ocenka effektivnosti investicij i innovacij v infocommunikaciyah* [Economic efficiency evaluation of investment and innovation in the infocommunications]. Moscow, ID Media Publisher, 2013. 250 p. (in Russian).

20. Azriliyan A. N. *Bolshoj ekonomicheskij slovar* [Big economics dictionary]. Moscow, Institut New Economics, 2002. 1280 p. (in Russian).

21. Adzhemov A. S., Buydinov E. V., Kuzovkova T. A. Primenenie integralnoj modeli dlya ocenki effectivnosti postroeniya sistemi sputnikovoj svyazi [Use of integral model for evaluation of the effectiveness of building the satellite communications system]. *Electrosvyaz*, 2016, vol. 4, pp. 25-29 (in Russian).

22. Bakanov M. I., Melnik M. V., Sheremet A. D. *Teoriya economicheskogo analiza* [Economic analysis theory]. Moscow, Financials and statistics Publ., 2005. 536 p. (in Russian).

23. Vertakova Y. V., Koziev I. A., Kuzbozhev E. N. *Upravlencheskie resheniya: razrabotka i vibor* [Management decisions: development and selection]. Moscow, KNORUS Publ., 2005. 352 p. (in Russian).

24. Sheremet A. D. *Teoriya ekonomicheskogo analiza* [Economic analysis theory]. Moscow, INFRA-M Publ., 2011. 352 p. (in Russian).

25. Azgaldov G. G. *Teoriya i praktika ocenki kachestva tovarov: Osnovi kvalimetrii* [Theory and practice of quality rating of goods: Qualimetry basics]. Moscow, Economics Publ., 1982. 256 p. (in Russian).

26. Volkov V. I. *Osnovi teorii i praktiki ekspertnoj deyatelnosti* [Basics of expert activities theory and practice]. Moscow, Academy of Innovation Management Publ., 2002. 196 p. (in Russian).

27. Kuzovkov D. V. Primenenie ekspertno-kvalimetricheskogo podhoda k ocenke effectivnosi innovacij i viboru postavschika oborudovaniya v sfere infokommunikacij [Use of expert-qualimetric approach to efficiency evaluation of innovations and selection of equipment suppliers in the field of Infocommunications]. *Vek Kachestva*, 2009, vol. 1, pp. 30-33 (in Russian).

28. Litvak B. G. *Ekspertnie tehnologii v upravlenii* [Expert technologies in management]. Moscow, Delo Publ., 2004. 400 p. (in Russian).

29. Mazur I. I., Shapiro V.D. *Upravlenie kachestvom* [Quality management]. Moscow, Publishing House "Omega-L", 2008. 399 p. (in Russian).

30. Fomin V. N. *Kvalimetriya. Upravlenie kachestvom. Sertifikaciya* [Qualimetry. Qualuity management. Sertifications]. Moscow, Os-89 Publ., 2007. 384 p. (in Russian).

31. Azgaldov G. G., Kostin A. V., Sadovov V. V. *Kvalimetriya: pervonachalnie svedeniya. Spravochnoe posobie s primerom dlya ANO "Agentstvo strategicheskih iniciativ po prodvidzeniyu novih proektov* [Qualimetry: the first information. Reference example for ANO "Strategic initiatives agency for promotion of new projects"]. Moscow, Visshaya shkola Publ., 2011. 143 p. (in Russian).

32. Adzhemov A. S., Buydinov E. V., Kuzovkov D. V. Primenenie ekspertno-kvalimetricheskogo metoda dlya obosnovaniya vibora effektivnih innovacij v sputnikovoj svyazi [Use of expert-qualimetric method to justify the selection of effective innovation in satellite communications]. *Elektrosvyaz*, 2015, vol. 1, pp. 27-30 (in Russian).

33. Tihvinskij V. O., Kuzovkov D. V. Ekspertno-kvalimetricheskij podhod k obosnovaniyu vibora innovacij I postavschikov v sfere innovacij [Expert-qualimetric approach to justify for the selection of innovations and equipment suppliers in zone of infocommunications]. *Vesnik RAEN*, 2009, vol. 3, pp. 58-64 (in Russian).

34. Malin A. S., Muhin V. N., *Issledovanie sistem upravleniya* [Research of management systems]. Moscow, HSE Publ., 2005. 399 p. (in Russian).

35. Kuzovkova T. A., Pronin A. M., Salutina T. Y., Tymoshenko L. S., Ustinova Y. S., Sharapova O. I. *Statistika sviazi* [Communications statistics]. Moscow: Radio and communication, 2003, 624 p. (in Russian).

36. *Gosudarstvennaia programma «Informatsionnoe obshchestvo (2011-2020 gody)»* [The state program "Information society (2011-2020)"], approved by order of the Government of the Russian Federation from October 20, 2010. № 1815-R (in Russian).

37. Kuzovkova T. A., Gencer M. A., Kuzovkov A. D. Metodicheskij apparat kompleksnogo prognozirovaniya razvitiya infokommunikacij [Methodological Apparatus of the Integrated Forecasting of the Development of Infocommunications]. *Systems of Control, Communication and Security*, 2016, vol. 1, pp. 146-190 (in Russian).

38. Salutina T. Y., Kuzovkov A. D. Kompleksnaya ocenka infokommunikacij I formirovaniya informacionnogo obschestva na osnove integralnogo I expertnogo metodov [Complex estimation of development and formation of telecommunications and information society based on integrated and expert methods]. *Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta sviazi i informatiki*

[Trudy Severo-Kavkazskiy branch of Moscow technical university of communications and informatics], Rostov-na-Donu, 2016, pp. 478-484 (in Russian).

39. *Indikatory informatsionnogo obshchestva: 2014* [Indicators information society: 2014]. Moscow, Research Institute "HSE" Publ., 2015, 320 p. (in Russian).

40. Karishev M. Y. Specifika primeneniya mezdunarodnoj statisticheskoj metodologii izmereniya informacionnogo obschestva v Rossii [The specific of usage of international statistical measurement the information society methodologies in Russia]. *Economics, Statistics and Informatics. Vesnik UMO*, 2011, vol. 4, pp. 89-92 (in Russian).

41. *Strategiya razvitiya FGUP "Kosmicheskaya Svyaz" na 2011-2015 godi i na period do 2020 g.* [Development strategy of FSUE "RSCC" on 2011-2015 and until 2020]. Moscow, GP KS, 2013. 278 p. (in Russian).

42. Postanovlenie Pravitel'stva Rossijskoj Federacii ot 21 aprelja 2014 g. № 366 "*Ob utverzhdenii gosudarstvennoj programmy Rossijskoj Federacii "Social'no-jekonomicheskoe razvitie Arkticheskoj zony Rossijskoj Federacii na period do 2020 goda"* [On approval of the state program of the Russian Federation "Socio-economic development of the Arctic zone of the Russian Federation for the period till 2020"] (in Russian).

Статья поступила 28 июня 2016 г.

Информация об авторах

Кузовкова Татьяна Алексеевна – доктор экономических наук, профессор кафедры экономики связи. Декан факультета экономики и управления. Московский технический университет связи и информатики. Область научных интересов: экономика, статистика, мониторинг, прогнозирование инфокоммуникаций. E-mail: tkuzovkova@me.com

Кузовков Дмитрий Валентинович – кандидат экономических наук, доцент кафедры экономики связи. Московский технический университет связи и информатики. Область научных интересов: экономика и развитие инфокоммуникаций, эффективность инноваций и инвестиций. E-mail: kuz_dim@mail.ru

Кузовков Александр Дмитриевич – аспирант кафедры экономики связи. Московский технический университет связи и информатики. Область научных интересов: экономика, статистика, прогнозирование инфокоммуникаций. E-mail: alexkuzovkov@mail.ru

Адрес: 111024, Россия, г. Москва, Авиамоторная ул., дом 8А.

Expert Qualimetry Method of Integral Estimation of Efficiency of Innovative Projects and New Technologies

T. A. Kuzovkova, D. V. Kuzovkov, A. D. Kuzovkov

Statement of the problem. *Development of new and improved methods of an integrated estimation of efficiency of innovative projects is relevant because of the high pace of the technological progress and development of infocommunications.**The aim of this paper** is the development and study of new method. This expert qualitative method for evaluating of effectiveness of innovations in the infocommunications field.* ***Method used. The*** *qualitative expert method based on the methods of qualimetry, the expert assessment methods, the statistical methods of analysis.* ***Novelty.*** *The novelty of the method is qualitative expert method used for to evaluate the efficiency of selecting useful innovations from a set of alternatives. The choice of the effective innovation based on quantitative measurement by experts the parameters of the innovation model and calculation of effectiveness factor in innovation.* ***Result.*** *This method for evaluating the innovation effectiveness can used to improve the degree of the decisions validity of social-economic management in the infotelecommunication field.* ***Practical significance.*** *This method proposes to used in the assessment of the innovative projects efficiency in the infocommunication companies. The method will allow to substantiate the more effective innovations which have the maximum socio-economic effects.*

Key words*: efficiency, innovation, innovative solutions, qualimetry, expert evaluation of the integral efficiency ratio, infocommunications.*

Information about Authors

Tatiana Alekseevna Kuzovkova – Dr. habil. of Economics Sciences. Professor of the Department of Economics of Communication. Dean of the faculty of Economics and Management. Moscow Technical University of Communications and Informatics. Research interests: Economics, statistics, monitoring, forecasting of infocommunications. E-mail: tkuzovkova@me.com

Dmitry Valentinovich Kuzovkov – Ph.D. of Economics Sciences, Associate Professor of the Department of Economics of communication. Moscow Technical University of Communications and Informatics. Research interests: Economics and development of infocommunications, efficiency of innovation and investment. E-mail: kuz_dim@mail.ru

Alexander Dmitrievich Kuzovkov – Doctoral Student of the Department of Economics of Communication. Moscow Technical University of Communications and Informatics. Research interests: Economics, statistics, forecasting of infocommunications. E-mail: alexkuzovkov@mail.ru

Address: Russia, 111024, Moscow, Aviamotornaya str., 8A.

УДК 519.711

Логико-математическое моделирование конфликтов

Левин В. И., Немкова Е. А.

Актуальность. *В статье рассмотрена актуальная проблема адекватного математического моделирования поведения конфликтующих систем, применительно к системам, конфликты в которых не обязательно связаны с антагонистическим противоречием между участниками системы. Дана формальная постановка задачи логико-математического моделирования процесса взаимодействия конфликтующих участников системы. Эта задача заключается в построении алгебр двузначной и многозначной логики, моделирующих различные типы мышления, различие которых и является источником конфликта.* ***Цель статьи.*** *Целью статьи является изложение и детальный анализ двузначной и многозначной логик, с упором на выяснение фундаментальных различий законов этих логик, влекущих за собой существенные различия в мышлении индивидов, базирующихся на указанных логиках, и вытекающие из этого различия конфликты между носителями различных логик мышления.* ***Метод.*** *Для решения поставленной задачи используется традиционный метод построения логических систем, основанный на введении базовых постоянных элементов, основных операций над ними и выявлении законов, которым подчиняются эти операции. При этом основное внимание уделяется различиям элементов операций над ними и законов операций между двузначной и многозначной логиками.* ***Новизна.*** *Сформулировано положение, согласно которому существуют системы, конфликты между участниками которых вызываются не антагонистическими противоречиями их интересов, а различием их логик мышления, следствием которого является непонимание, провоцирующее подозрительность, а потом и агрессию. Это так называемые воображаемые конфликты, борьба с которыми требует специальных подходов.* ***Результат.*** *Разработана процедура построения алгебры логики различной значности, адекватно моделирующей процессы мышления. Описаны двузначная и многозначная логики мышления и их законы. Установлены фундаментальные различия двузначной и многозначной логик. Приведен пример анализа конфликта, вызванного различием логик мышления.*

Ключевые слова: *конфликт, формальная логика, элементы, логические операции, законы логики, высказывание, двузначная логика, многозначная логика.*

Введение

Несомненна важность общей теории конфликта – науки, занимающейся расчетом, анализом, синтезом и разрешением общих моделей конфликтных ситуаций. В то же время ясно, что построение продуктивных моделей конфликта должно быть основано на привязке к наиболее важным конкретным классам конфликтующих систем. И самый большой интерес среди этих систем вызывает, конечно, человеческое общество.

Конфликтами в человеческом обществе с целью их практического разрешения в настоящее время занимается гуманитарная наука – конфликтология, являющаяся частью социологии. Однако эта наука не стремится вскрыть внутреннюю природу конфликтных ситуаций, а без этого невозможно построить соответствующие хорошие математические модели, позволяющие детально изучать такие ситуации.

Обычно считается, что источником человеческих конфликтов является противоречие между целями, которые различные люди ставят между собой [1-3]. Однако не секрет, что большая (а возможно, и подавляющая) часть человечества – это люди, которые не ставят перед собой никаких особых целей.

Но при этом они часто конфликтуют с другими людьми – как бесцельно существующими, подобными им, так и с вполне целеустремленными людьми. Этот факт побуждает предполагать, что в основе конфликтов между людьми лежит еще и какая-то другая особенность человеческой личности, не связанная напрямую с деятельностью человека и его целями, а присущая ему на генетическом уровне. В настоящей статье выдвигается и обосновывается гипотеза, согласно которой особенность человека, которая сильно, а иногда решающим образом влияет на возникновение (или отсутствие) его конфликтов с окружающими, это тип, а точнее – логика его мышления. С этой целью рассматриваются два существенно различных типа логики – двузначная и многозначная, а затем показывается, что основанные на них варианты человеческого мышления в значительной мере несовместимы. Эта несовместимость и приводит к взаимонепониманию между приверженцами двух указанных типов мышления и, в конечном счете, к конфликтам между ними.

1. Двузначная формальная логика

Двузначная формальная (иначе – математическая, символическая) логика высказываний, называемая еще классической, лежит в основе обычного человеческого мышления. Эта логика строится с помощью двух постоянных элементов: ИСТИНА (обозначение И) и ложь (обозначение Л); переменных, значениями которых служат значения истинности различных высказываний, и логических операций, которые можно выполнять над постоянными элементами. Высказывание – это утверждение, которое может быть либо истинным (И), либо ложным (Л). Поэтому логические операции можно выполнять и над высказываниями. Логические операции над постоянными элементами или высказываниями P,Q следующие: отрицание $\overline{P}$ (иначе «НЕ P»), дизъюнкция $P \vee Q$ (иначе «P ИЛИ Q»), конъюнкция $P \wedge Q$ (иначе «P И Q»), разделительная дизъюнкция $P \oplus Q$ (иначе «ЛИБО P, ЛИБО Q»), эквивалентность $P \leftrightarrow Q$ (иначе «P РАВНОСИЛЬНО Q»), импликация $P \rightarrow Q$ (иначе «ЕСЛИ P, ТО Q»). Эти операции определены в таблицах истинности 1 и 2. Кроме высказываний, имеющих переменные значения истинности (И или Л), имеются два высказывания с постоянными значениями истинности: тождественно истинное высказывание или тавтология (обозначение Т) и тождественно ложное высказывание или противоречие (обозначение П).

Таблица 1 – Операция отрицания

P	$\overline{P}$
И	Л
Л	И

Таблица 2 – Операции дизъюнкции, конъюнкции, разделительной дизъюнкции, эквивалентности и импликации

P	Q	$P \vee Q$	$P \wedge Q$	$P \oplus Q$	$P \leftrightarrow Q$	$P \rightarrow Q$
Л	Л	Л	Л	Л	И	И
И	Л	И	Л	И	Л	Л
Л	И	И	Л	И	Л	И
И	И	И	И	Л	И	И

Во введенной логике справедливы следующие законы:

- переместительный закон для дизъюнкции и конъюнкции
$$P \vee Q = Q \vee P, \quad P \wedge Q = Q \wedge P; \tag{1}$$
- сочетательный закон для дизъюнкции и конъюнкции
$$(P \vee Q) \vee R = P \vee (Q \vee R), \quad (P \wedge Q) \wedge R = P \wedge (Q \wedge R); \tag{2}$$
- распределительный закон для конъюнкции относительно дизъюнкции
$$(P \vee Q) \wedge R = (P \wedge R) \vee (Q \wedge R); \tag{3}$$
- распределительный закон для дизъюнкции относительно конъюнкции
$$(P \wedge Q) \vee R = (P \vee R) \wedge (Q \vee R); \tag{4}$$
- закон де Моргана
$$\overline{P \vee Q} = \overline{P} \wedge \overline{Q}, \quad \overline{P \wedge Q} = \overline{P} \vee \overline{Q}; \tag{5}$$
- закон тавтологии
$$P \vee P = P, \quad P \wedge P = P; \tag{6}$$
- закон поглощения
$$P \wedge (P \vee Q) = P, \quad P \vee (P \wedge Q) = P; \tag{7}$$
- закон действия над высказываниями с постоянными значениями истинности
$$P \vee \Pi = P, \quad P \vee \mathrm{T} = \mathrm{T}, \quad P \wedge \mathrm{T} = P, \quad P \wedge \Pi = \Pi; \tag{8}$$
- закон двойного отрицания
$$\overline{\overline{P}} = P; \tag{9}$$
- закон исключенного третьего
$$P \vee \overline{P} = \mathrm{T}; \tag{10}$$
- закон противоречия
$$P \wedge \overline{P} = \Pi; \tag{11}$$
- закон преобразования импликации
$$(P \rightarrow Q) = \overline{P} \vee Q. \tag{12}$$

Для доказательства законов двузначной логики строятся таблицы истинности их обеих частей, подобные табл. 1, 2. Если оказывается, что таблицы для обеих частей совпадают, то закон справедлив. Логические законы позволяют заменять выражения логики высказываний эквивалентными, но более простыми (либо более удобными в каком-то смысле) выражениями.

Построенная логика высказываний позволяет формально описывать процесс человеческого мышления, используя формальную конструкцию

$$A_1 \wedge A_2 \wedge ... \wedge A_n \to B\,. \qquad (13)$$

Здесь $A_1,...,A_n$ – исходные высказывания (посылки), B – новое высказывание (заключение). Сложное высказывание (13) называется логическим выводом. Логический вывод может быть истинным или ложным. Если он истинен при любых значениях истинности посылок и заключения (т.е. тождественно истинен), он считается верным. В остальных случаях логический вывод считается неверным. Для проверки верности логического вывода можно построить его таблицу истинности и убедиться, что он тождественно истинен либо преобразовать выражение (13) логического вывода с помощью подходящих логических законов и привести его к тождественно истинному высказыванию.

Приведем еще один логический закон – транзитивности импликации, важный для логического вывода

$$(P \to Q) \wedge (Q \to R) \to (P \to R)\,. \qquad (14)$$

Закон (14) показывает, что операция импликации $\to$ транзитивна, что позволяет осуществлять логический вывод как многоступенчатый (цепочечный) процесс.

Двузначная формальная логика и реализующие ее автоматы широко используются для математического моделирования многих классов систем. В частности, конфликтующих систем [4-12].

2. Многозначная формальная логика

Все основные черты многозначной логики проявляются, начиная со значности $k = 3$. Поэтому ограничимся трехзначной формальной логикой высказываний. Эта логика лежит в основе человеческого мышления, более сложного, чем обычное. Она строится с помощью тех же постоянных элементов, что и двузначная логика: И и Л, с добавлением постоянного элемента НЕОПРЕДЕЛЕННОСТЬ (обозначение Н). Новый элемент является неопределенностью в том смысле, что он не истинен и не ложен. Как и в двузначной логике, в качестве переменных значений используется истинность различных высказываний. Эти значения теперь могут быть И, Л или Н. Логические операции можно выполнять над постоянными элементами И, Л и Н и над переменными (высказываниями), принимающими эти же значения И, Л и Н. В трехзначной логике имеются те же операции, что и в двузначной. Однако число возможных вариантов каждой операции значительно больше. В табл. 3-5 определены три наиболее употребительных варианта операции отрицания. В табл. 6 определены операции дизъюнкции $P \vee Q$, конъюнкции $P \wedge Q$, разделительной дизъюнкции $P \oplus Q$, эквивалентности $P \leftrightarrow Q$, импликации $P \to Q$ (по одному варианту для каждой операции). Кроме высказываний с переменными значениями истинности (И, Л или Н), имеются три высказывания с постоянными значениями истинности: И (называемое тавтологией Т), Л (называемое противоречием П) и Н (называемое неопределенностью Н).

Первые две совпадают с соответствующими в двузначной логике, третье является новым высказыванием с постоянным значением истинности.

Таблица 3 – Зеркальное отрицание

P	$\overline{P}$
И	Л
Н	Н
Л	И

Таблица 4 – Левое циклическое отрицание

P	$\overline{P}$
И	Н
Н	Л
Л	И

Таблица 5 – Правое циклическое отрицание

P	$\overline{P}$
И	Л
Н	И
Л	Н

Таблица 6 – Операции дизъюнкции, конъюнкции, разделительной дизъюнкции, эквивалентности и импликации

P	Q	$P \vee Q$	$P \wedge Q$	$P \oplus Q$	$P \leftrightarrow Q$	$P \to Q$
Л	Л	Л	Л	Л	И	И
Л	Н	Н	Л	Н	Н	И
Л	И	И	Л	И	Л	И
Н	Л	Н	Л	Н	Н	Н
Н	Н	Н	Н	Н	Н	Н
Н	И	И	Н	Н	Н	И
И	Л	И	Л	И	Л	Л
И	Н	И	Н	Н	Н	Н
И	И	И	И	Л	И	И

Во введенной трехзначной логике остаются справедливы законы двузначной логики, не содержащие операции отрицания. Это законы переместительный, сочетательный и распределительный (1)–(4), тавтологии, поглощения и действий с постоянными (6)–(8), транзитивности (14). Однако появляются новые законы действий над высказываниями с постоянным значением истинности Н

$$\text{Н} \vee \text{Л} = \text{Н}, \quad \text{Н} \vee \text{И} = \text{И}, \quad \text{Н} \wedge \text{Л} = \text{Л}, \quad \text{Н} \wedge \text{И} = \text{Н}. \qquad (15)$$

Главное же отличие трехзначной логики от двузначной состоит в существенном изменении законов, содержащих операцию отрицания. Конкретный вид этих законов зависит от выбранного варианта операции отрицания. Если это операция зеркального отрицания (табл. 3), то остаются

справедливыми законы де Моргана, двойного отрицания и преобразования импликации (5), (9), и (12) двузначной логики, однако закон исключенного третьего (10) переходит в следующий закон «частично исключенного третьего»

$$P \vee \overline{P} = \mathrm{T}'(P), \quad \text{где} \quad \mathrm{T}'(P) = \begin{cases} \text{И}, & \text{при } P = \text{И или Л}; \\ \text{Н}, & \text{при } P = \text{Н}; \end{cases} \tag{16}$$

а закон противоречия (11) – в следующий закон «частичного противоречия»

$$P \wedge \overline{P} = \Pi'(P), \quad \text{где} \quad \Pi'(P) = \begin{cases} \text{Л}, & \text{при } P = \text{И или Л}; \\ \text{Н}, & \text{при } P = \text{Н}. \end{cases} \tag{17}$$

Для операций левого и правого циклического отрицания (табл. 4 и 5) все законы двузначной логики, содержащие отрицание, трансформируется в соответствующие новые, более сложные законы трехзначной логики. Так, законы двойного отрицания (9), исключенного третьего (10) и противоречия (11) трансформируется в соответствующие законы – закон тройного отрицания

$$\overline{\overline{\overline{P}}} = P, \tag{18}$$

закон исключенного четвертого

$$P \vee \overline{P} \vee \overline{\overline{P}} = \mathrm{T} \tag{19}$$

и закон полного противоречия

$$P \wedge \overline{P} \wedge \overline{\overline{P}} = \Pi, \tag{20}$$

а законы де Моргана (5) и преобразования импликации (12) – в соответствующие более сложные законы, форма которых уже зависит от того, какое циклическое отрицание использовано – левое или правое. В связи с обсуждаемой проблемой логики мышления особое значение имеет конкретизация закона (18) в виде

$$\overline{\overline{\overline{P}}} \neq P, \ \forall P; \tag{21}$$

закона (19) в виде закона «частично исключенного третьего»

$$\left.\begin{array}{l} P \vee \overline{P} = \mathrm{T}^{\text{л}}(P), \quad \text{где} \quad \mathrm{T}^{\text{л}}(P) = \begin{cases} \text{И}, & \text{при } P = \text{И или Л}, \\ \text{Н}, & \text{при } P = \text{Н}, \end{cases} \\ \text{для левого циклического отрицания;} \\ P \vee \overline{P} = \mathrm{T}^{\text{п}}(P), \quad \text{где} \quad \mathrm{T}^{\text{п}}(P) = \begin{cases} \text{И}, & \text{при } P = \text{И или Н}, \\ \text{Н}, & \text{при } P = \text{Л}, \end{cases} \\ \text{для правого циклического отрицания;} \end{array}\right\} \tag{22}$$

и закона (20) в виде закона «частичного противоречия»

$$\left.\begin{array}{l} P \wedge \overline{P} = \Pi^{\text{л}}(P), \quad \text{где} \quad \Pi^{\text{л}}(P) = \begin{cases} \text{Л}, & \text{при } P = \text{Л или Н}, \\ \text{Н}, & \text{при } P = \text{И}, \end{cases} \\ \text{для левого циклического отрицания;} \\ P \wedge \overline{P} = \Pi^{\text{п}}(P), \quad \text{где} \quad \Pi^{\text{п}}(P) = \begin{cases} \text{Л}, & \text{при } P = \text{Л или И}, \\ \text{Н}, & \text{при } P = \text{Н}, \end{cases} \\ \text{для правого циклического отрицания.} \end{array}\right\} \tag{23}$$

Как видно из (21), в трехзначной логике с операцией циклического отрицания не действует закон двойного отрицания. Далее, из (22) следует, что в этой логике не действует закон исключенного третьего – он трансформируется

в закон «частично исключенного третьего», конкретная форма которого зависит от варианта операции циклического отрицания (правое или левое). Аналогично, из (23) следует, что в этой логике не действует закон противоречия – он трансформируется в закон «частичного противоречия», конкретная форма которого также зависит от варианта операции циклического отрицания.

3. Логика и конфликты

Каждый мыслящий индивидуум в своей мыслительной деятельности всегда использует сознательно или интуитивно тот или иной вариант логики. Выше мы видели, что между двузначной и многозначной логиками есть существенные различия. Поэтому всех индивидуумов, по используемому в их мышлении преимущественного варианту логики, можно разделить на двузначных и многозначных мыслителей. Их основные различия заключаются в том, что для двузначного мыслителя любое высказывание может иметь только два значения истинности: истинно и ложно, причем отрицание одного дает другое, в то время как для многозначного мыслителя любое высказывание имеет, как минимум, три значения истинности: истинно, ложно и неопределенно. При этом операция отрицания может быть определена по-разному, так что отрицание любого значения истинности в общем случае может дать любое другое значение истинности.

Ввиду указанных глубоких различий между двузначными и многозначными мыслителями возникает сложная проблема их взаимоотношений. Сущность этой проблемы в том, что в рамках двузначного мышления трудно понять явно многозначную природу мира (с точки зрения современной науки). Такое постоянное недопонимание ведет к подозрительности и страху. В итоге двузначный мыслитель начинает конфликтовать с многозначным, склоняясь к силовому решению.

Рассмотрим простейший характерный пример. На банкете, во время застолья, художник, уже изрядно навеселе обращается к ученому: «Ты что не пьешь?» – Тот отвечает: «Не могу!». Художник продолжает настаивать: «Пей!». Ученый возражает: «Не буду!». Тогда художник заявляет громогласно: «Значит, ты собираешься написать на нас донос!». Наш художник, конечно типичный двузначный мыслитель, для которого существует лишь два варианта: пить и потому быть не способным донести и не пить и потому быть способным написать донос. Ему не приходит в голову, что есть и другие варианты, очевидные для ученого – многозначного мыслителя. Например, напиться до беспамятства, а потом донести о том чего не было, или вообще не пить и при этом не доносить из нравственных соображений.

Реальная версия этой полуфантастической истории произошла в 1938 году на правительственной даче в Кунцево, под Москвой, когда во время очередного банкета, устроенного И.В. Сталиным, ему не удалось заставить пить наркома кинематографии СССР Бориса Шумяцкого. После чего по приказу двузначного мыслителя Сталина подозрительный многозначный мыслитель Шумяцкий был расстрелян.

Изложенные в данном разделе соображения могут быть положены в основу нового многозначно-логического подхода к моделированию конфликтов, отличного от двузначно-логического подхода, основанного на математическом аппарате, рассмотренном в работе [12]. Такой новый подход открывает новые перспективы моделирования конфликтов. В частности, он позволит увеличить число градаций взаимодействия конфликтующих систем и тем самым сделает анализ этого взаимодействия более тонким. Подробное изложение данного подхода предполагается в отдельной статье.

Заключение

В статье показано, что двузначная и многозначная логики подчиняются существенно различным законам, благодаря чему могут быть использованы для моделирования различных типов мышления. Выявлено, что источником человеческих конфликтов может быть не только противоречие между целями, которые различные люди ставят перед собой, но и человеческое взаимонепонимание, вызванное различием типов мышления. Достоинство описываемого подхода к изучению конфликтов заключается в возможности более тонкого проникновения в суть развития конфликтных ситуаций.

Литература

1. Дмитриев А. В. Конфликтология. – М.: ИНФРА–М, 2009. – 336 с.

2. Сысоев В. В. Конфликт. Сотрудничество. Независимость: системное взаимодействие в структурно-параметрическом представлении. – Москва: МАЭиП, 1999. – 151 с.

3. Светлов В. А. Аналитика конфликта. – СПб: Росток, 2001. – 512 с.

4. Левин В. И. Математическое моделирование систем с помощью динамических автоматов // Информационные технологии. 1997. № 9. С. 15-24.

5. Левин В. И. Математическое моделирование с помощью автоматов // Вестник Тамбовского университета. Серия: Естественные и технические науки. 1997. Т. 2. № 2. С. 67-72.

6. Левин В. И. Автоматная модель определения возможного времени проведения коллективных мероприятий // Известия РАН. Теория и системы управления. 1997. № 3. С. 85-96.

7. Левин В. И. Математическое моделирование библии. Характеристический автоматный подход // Вестник Тамбовского университета. Серия: Естественные и технические науки. 1999. Т. 4. № 3. С. 353–363.

8. Левин В. И. Автоматное моделирование коллективных мероприятий // Автоматика и телемеханика. 1999. № 12. С. 78-89.

9. Левин В. И. Математическое моделирование библейской легенды о Вавилонском столпотворении // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2001. Т. 6. № 2. С. 123-138.

10. Левин В. И. Автоматное моделирование исторических процессов на примере войн // Радиоэлектроника. Информатика. Управление. 2002. № 12. С. 93-101.

11. Левин В. И. Автоматное моделирование процессов возникновения и распада коллектива // Кибернетика и системный анализ. 2003. № 3. С. 92-101.

12. Левин В. И. Логико-алгебраический подход к моделированию конфликтов // Системы управления, связи и безопасности. 2015. № 4. С. 69-87. URL: http://sccs.intelgr.com/archive/2015-04/03-Levin.pdf (дата обращения 01.08.2016).

References

1. Dmitriev A .V. *Konfliktologiia* [Conflictology]. Moscow, INFRA-M Publ., 2009. 336 p. (in Russian).

2. Sysoev V. V. *Konflikt. Sotrudnichestvo. Nezavisimost': sistemnoe vzaimodeistvie v strukturno-parametricheskom predstavlenii* [Conflict. Cooperation. Independence: the systemic interaction of structural and parametric representation]. Moscow, MAEP Publ., 1999. - 151 p. (in Russian).

3. Svetlov V. A. *Analitika konflikta* [Analysis of the conflict]. Saint-Petersburg, Burgeon Publ., 2001. 512 p. (in Russian).

4. Levin V. I. Mathematical modeling of systems with dynamic machines. *Information technologies,* 1997, no. 9, pp. 15-24 (in Russian).

5. Levin V. I. Mathematical modeling using automata. *Bulletin of the University of Tambov. Series: Natural and Technical Sciences,* 1997, vol. 2, no. 2, pp. 67-72. (in Russian).

6. Levin V. I. Automaton model determine the possible time of the collective actions. *Izvestiya RAS. Theory and control systems,* 1997, no. 3, pp. 85-96. (in Russian).

7. Levin V. I. Mathematical modeling of the Bible. Characteristic automata approach. *Bulletin of the University of Tambov. Series: Natural and Technical Sciences,* 1999, vol. 4, no. 3, pp. 353-363 (in Russian).

8. Levin V. I. Automatic modeling of collective actions. *Automation and Remote Control*, 1999, no. 12, pp. 78-89 (in Russian).

9. Levin V. I. Mathematical modeling of the biblical legend of the Tower of Babel. *Bulletin of the University of Tambov. Series: Natural and Technical Sciences,* 2001, vol. 6, no 2, pp. 123-138 (in Russian).

10. Levin V. I. Automatic modeling of historical processes on the example of the wars. *Electronics. Computer science. Control,* 2002, no. 12, pp. 93-101 (in Russian).

11. Levin V. I. Automatic modeling of processes of emergence and collapse of collective // *Cybernetics and Systems Analysis,* 2003, no. 3, pp. 92-101 (in Russian).

12. Levin V. I. Logical-Algebraic Approach to Conflicts Modeling. *Systems of Control, Communication and Security,* 2015, no. 4, pp. 69-87. Available at: http://sccs.intelgr.com/archive/2015-04/03-Levin.pdf (accessed 01 Aug 2016) (in Russian).

Статья поступила 19 июля 2016 г.

Информация об авторах

Левин Виталий Ильич – доктор технических наук, профессор, PhD, Full Professor. Заслуженный деятель науки РФ. Пензенский государственный технологический университет. Область научных интересов: логика;

математическое моделирование в технике, экономике, социологии, истории; принятие решений; оптимизация; теория автоматов; теория надежности; распознавание; история науки; проблемы образования. E-mail: vilevin@mail.ru

Немкова Елена Анатольевна – кандидат технических наук, доцент кафедры «Математика». Пензенский государственный технологический университет. Область научных интересов: логика; математическое моделирование в технике и экономике. E-mail: elenem58@mail.ru

Адрес: 440039, Россия, г. Пенза, пр. Байдукова/ул. Гагарина, д. 1а/11.

Logical-Mathematical Modelling of Conflicts

V. I. Levin, E. A. Nemkova

Relevance. *In the article the actual problem of adequate mathematical modeling of the behavior of the conflicting systems in relation to systems, conflicts are not necessarily related to the contradiction between the participants in the system. An exact statement of the problem of logical and mathematical modeling of the interaction between the conflicting parties of the system. The task is to build a two-valued algebra and multi-valued logic, simulating different types of thinking, and that difference is a source of conflict.* ***The purpose of the article.*** *The aim of the article is a summary and a detailed analysis of the two-valued and multi-valued logic, with a focus on finding the fundamental differences of the laws of logic, entailing significant differences in the thinking of individuals, based on these logics and the resulting differences in conflicts between carriers of different logics of thinking.* ***Method****. To solve this problem, we use the traditional method of construction of logical systems based on the introduction of basic elements of permanent, major operations on them and identify the laws that govern these operations. The main attention is paid to the differences of elements of operations on them and transactions between the laws of two-valued and multi-valued logic.* ***Novelty****. Formulated provision according to which there are systems, conflicts between the parties which are not caused by the contradictions of their interests and the difference of their logic thinking, the result of which is a misunderstanding, provoking suspicion, and then aggression. This so-called imaginary conflicts, the fight against which requires special approaches.* ***Result.*** *The procedure of constructing the algebra of logic different valence, adequately modeling the processes of thinking. We describe the two-valued and multi-valued logic thinking and their laws. Established the fundamental differences of two-valued and multi-valued logic. An example of the analysis of the conflict caused by the difference logic thinking.*

Keywords*: conflict, formal logic elements, logic operations, the laws of logic, statement, the two-valued logic, many-valued logic.*

Information about Authors

Vitaly Ilyich Levin – the Doctor of Engineering Sciences, Professor, PhD, Full Professor. Honored worker of science of the Russian Federation. Penza State Technological University. Field of Research: logic; mathematical modeling in technics, economy, sociology, history; decision-making; optimization; automata theory; theory of reliability; history of science; problems of education. E-mail: vilevin@mail.ru

Elena Anatolyevna Nemkova – Ph.D. of Engineering Sciences, Associate Professor at the Department of "Mathematics". Penza State Technological University. Field of Research: logic; mathematical modeling in technics, economy. E-mail:: elenem58@mail.ru

Address: 440039, Russia, Penza, pr. Baydukova / Gagarin st., 1a/11.

УДК 622.232.8:621.384.3.01:531.714.2

Высокочувствительные телевизионные камеры для обеспечения безопасности

Волков В. Г.

Постановка задачи: *рассматриваются новые высокочувствительные телевизионные (ТВ) камеры для обеспечения работы служб безопасности. Показаны их возможности, описаны технические параметры.* ***Цель работы:*** *показать последние достижения в области создания конкретных ТВ камер различного типа для обеспечения безопасности.* ***Используемые методы:*** *сравнительный научно-технический анализ возможностей ТВ камер и вопросов их применения в системах обеспечения безопасности.* ***Новизна:*** *впервые показаны в систематизированном виде технические параметры высокочувствительных ТВ камер для устройств обеспечения безопасности. Все ТВ камеры выполнены либо в виде портативных, либо стационарных устройств.* ***Практическая значимость:*** *показана эффективность и перспективность применения высокочувствительных ТВ камер в системах обеспечения безопасности благодаря их высоким параметрам, возможности обеспечения круглосуточного наблюдения и работы в ухудшенных условиях видения.*

Ключевые слова: *ТВ камера, чувствительность, отношение сигнал/шум, разрешение, динамический диапазон, размер пикселя, размер активной области, масса, габариты, энергопотребление.*

Актуальность

В настоящее время большой интерес проявляется к созданию высокочувствительных телевизионных (ТВ) камер для специальной техники [1-5]. На основе таких ТВ камер созданы высокоэффективные низкоуровневые телевизионные системы [1-3]. Они предназначены для широкого применения в службах обеспечения безопасности: охрана объектов методом патрулирования или стационарным методом, обеспечения работы пограничных, таможенных служб, служб МВД и МЧС, для работы бойцов спецподразделений, разведки.

Методы повышения чувствительности ТВ камер с использованием традиционных матриц ПЗС

Для повышения чувствительности ТВ камер могут быть использованы следующие варианты [1-5]:

1) охлаждение матриц ПЗС;
2) повышение чувствительности за счет применения растровой оптики и светосильных объективов,
3) использование так называемых ночных режимов № 1 и № 2,
4) применение гибридно-модульных преобразователей изображения,
5) использование матриц ПЗС с электронным умножением.

Известно, что охлаждение матрицы ПЗС на каждые 9°С приводит к уменьшению ее темнового тока в 2 раза [2]. Поэтому применяют охлаждение матриц ПЗС путем заливки жидкого азота в сосуд Дьюара, в котором смонтирована матрица. При этом температура охлаждения составляет 77 К. Чаще используют охлаждение с помощью одно- или двухкаскадных

термоэлектрических охладителей (ТЭО). Но такие технические решения не получили широкого распространения.

Применение растровой оптики – микролинзы на каждом пикселе (рис. 1) позволяет увеличить охват излучение и в сочетании со светосильными объективами на входе ТВ камеры (относительное отверстие 1:0,8 вместо 1:1,2 или 1:1,4) повысить соответственно чувствительность матрицы ПЗС.

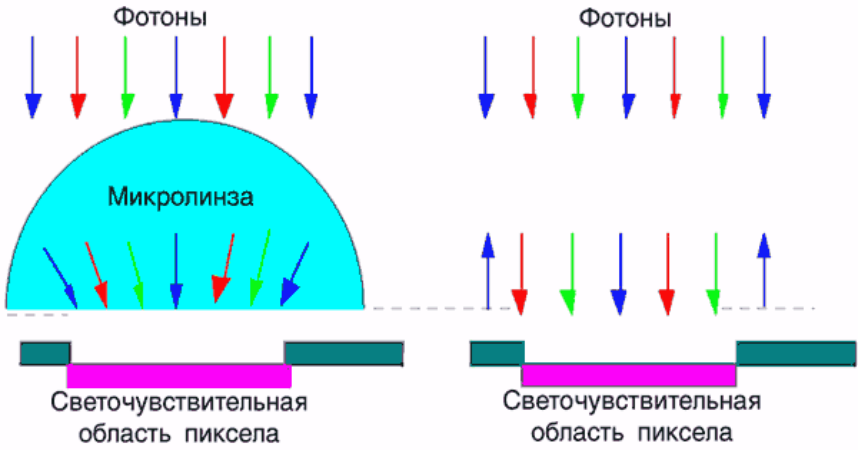


Рис. 1. Применение растровой оптики – микролинзы на каждом пикселе позволяет увеличить охват излучение

Фирма Sony повысила чувствительность матриц ПЗС EXview приблизительно в 4 раза за счет повышения величины абсолютной чувствительности и ее сдвига в ближнюю инфракрасную (ИК) область спектра.

Созданы новые типы матриц ПЗС HAD CCD, которые имеют отношение сигнал/шум свыше 115 дБ по сравнению с 20 дБ, для обычных матриц ПЗС [2]. На рис. 2 представлены кривые спектральной чувствительности обычной матрицы ПЗС фирмы Sony (ICX058CL) EXview HAD CCD (ICX258AL) [1, 2].

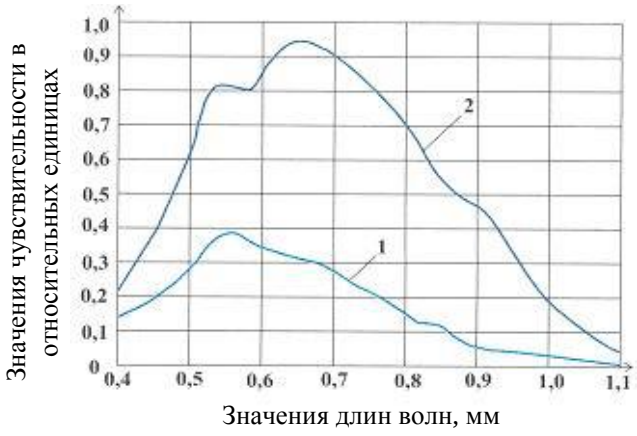


Рис. 2. Сравнительные спектральные характеристики:
кривая 1 – обычная матрица ПЗС, модель ICX058CL фирмы Sony;
кривая 2 – матрица EXview HAD CCD, модель ICX258AL той же фирмы

Конкретным примером таких ТВ камер могут служить модели фирмы Watec Ltd (Япония) (таблица 1 приложения) – рис. 3. Однако чувствительность таких ТВ камер все еще сравнительно не высока.

а. б.

Рис. 3. ТВ камеры фирмы Watec Ltd.:
а – в корпусном; б – в бескорпусном исполнении

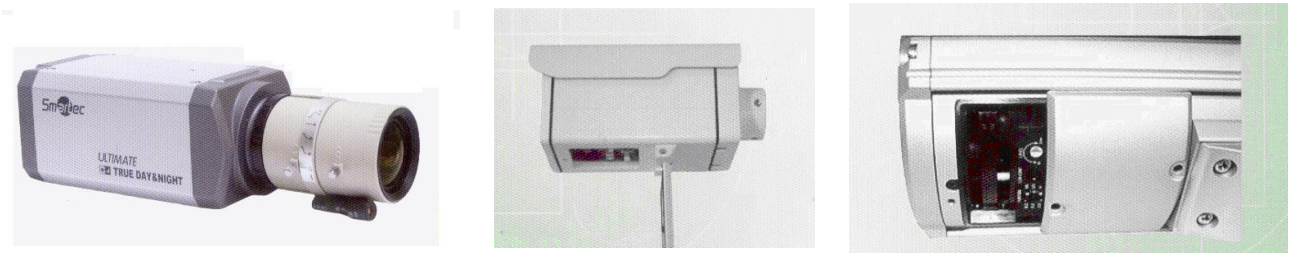
Фирме Sony удалось достичь оптимизации стыковки пикселя и микролинзы и разработать новую матрицу ПЗС Super HAD CCD II с улучшенной структурой. При этом была обеспечена чувствительность от 1000 мВ на квадратный микрон относительно отверстие объектива 1:5,6 для цветных сенсоров и 1:8 для черно-белых, время накопления 1 с. Это позволило расширить динамический диапазон сенсора на 6 дБ. Фирме удалось также добиться уменьшения расфокусировки, которое происходит при использовании объективов без ИК коррекции [6].

Более того, область фоточувствительного слоя пикселя была увеличена. Это привело к высокой эффективности преобразования оптического сигнала в электрический сигнал. В этой матрице ПЗС улучшилась цветопередача. За счет применения нового химического состава наносимых цветных пигментных элементов повысилась чувствительность в синей части рабочей области спектра, а также были достигнуты сбалансированные показатели спектральной чувствительности. Благодаря этому удалось снизить уровень шумов цветности. Сохранена высокая устойчивость к засветкам характерная для предыдущих моделей матриц ПЗС (Super HAD, Exview HAD). За счет механически отключаемого ИК фильтра реализован режим «День/Ночь». При этом минимальная рабочая освещенность в цветном режиме составляет до 0,15 лк, а в черно-белом режиме – до 10^{-3} лк (при относительном отверстии объектива 1:1,2). За счет оптимизации цифровой обработки сигнала в ТВ камерах достигнуто разрешение 580 ТВ линий в цветном и 700 ТВ линий в черно-белом режиме. Используется при этом функция подавления шумов (SSNR3) в условиях пониженной освещенности. При настройке предоставляется возможность выбора одного из 32 уровней подавления шумов. При этом достигается экономия на 70% дискового пространства видеорегистратора при

записи видеосигнала от ТВ камеры, т.к. шумы воспринимаются видеорегистратором как дополнительные элементы изображения и не могут быть подвергнуты эффективной компрессии. Для устранения дрожания изображения, возникающего при установке ТВ камер в условиях для наружного наблюдения (например, из-за проезжающего мимо большегрузного транспорта), предусмотрена цифровая стабилизация изображения (DIS). Инверсия ярких засветок связана с возможностью процессора цифровой обработки сигнала затемнять особо яркие участки кадра. Это существенно улучшает различимость прилегающих к ним участков изображения. Данный режим полезен, например, для распознавания номерных знаков автомобилей с включенными фарами. Режим расширенного динамического диапазона (SSDR) позволяет использовать ТВ камеры в условиях присутствия в зоне наблюдения как хорошо, так и плохо освещенных объектов одновременно. SSDR подавляет особо яркие участки изображения и улучшает контраст для слабо освещенных деталей [6].

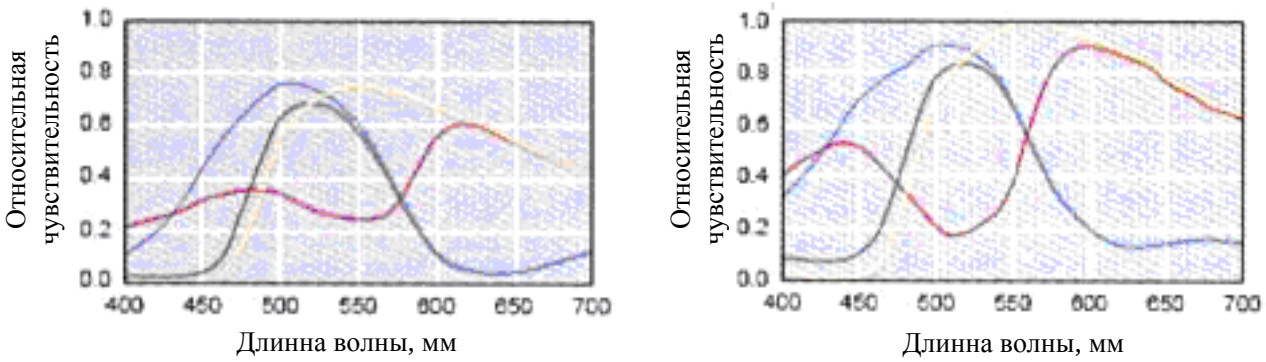
Режим суммирования кадров (кадрового накопления) (DSS) позволяет существенно повысить чувствительность ТВ камеры в условиях пониженного уровня освещенности. Например, при суммировании 256 кадров минимальная рабочая освещенность составляет 4×10^{-5} лк в черно-белом режиме (относительное отверстие объектива – 1:1,2). Максимальное количество суммируемых кадров можно настроить из меню. В процессе настройки можно выбрать любой из 14 языков интерфейса, включая русский. Предусмотрен детектор движения и настройка 8 его зон при детектировании движения, для каждой из которых может быть индивидуально определена чувствительность [6].

На рис. 4 представлен внешний вид таких ТВ камер, а на рис. 5-11 наглядно иллюстрируются их возможности.



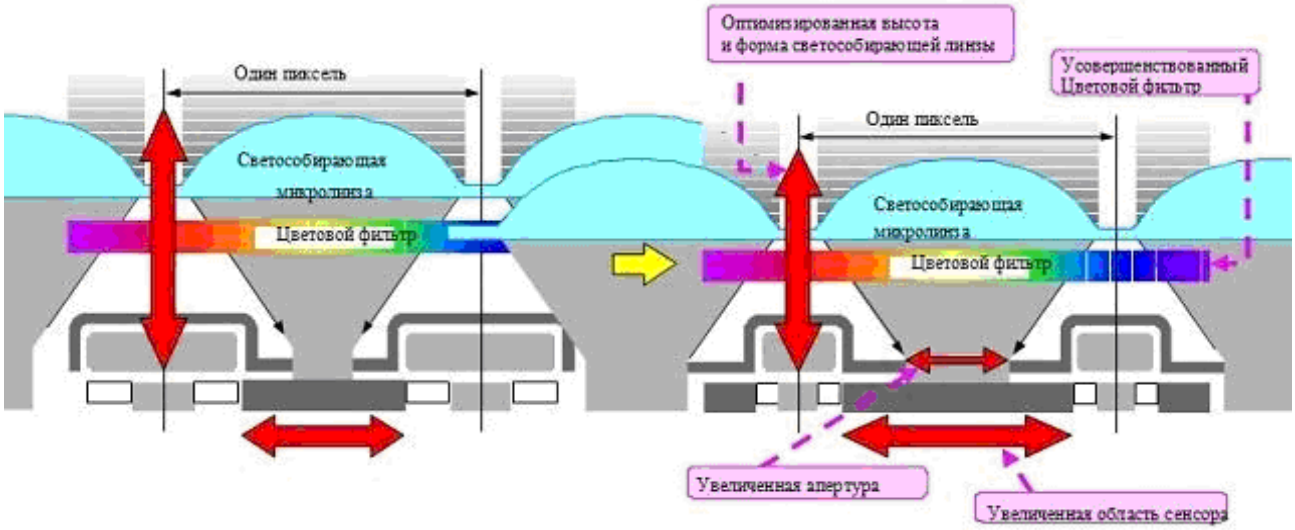
а. б. в.

Рис. 4. Внешний вид ТВ камер на основе матриц ПЗС Super HAD CCD II:
а – STC-3080; б – STC-3630 ULTIMATE; в – STC-3680 ULTIMATE



а. б.

Рис. 5. Сравнение характеристик спектральной чувствительности матриц ПЗС Super HAD CCD и Super HAD CCD II



а. Super HAD CCD б. Super HAD CCD II

Рис. 6. Изменения в матрице Super HAD CCD II, которые привели к повышению чувствительности

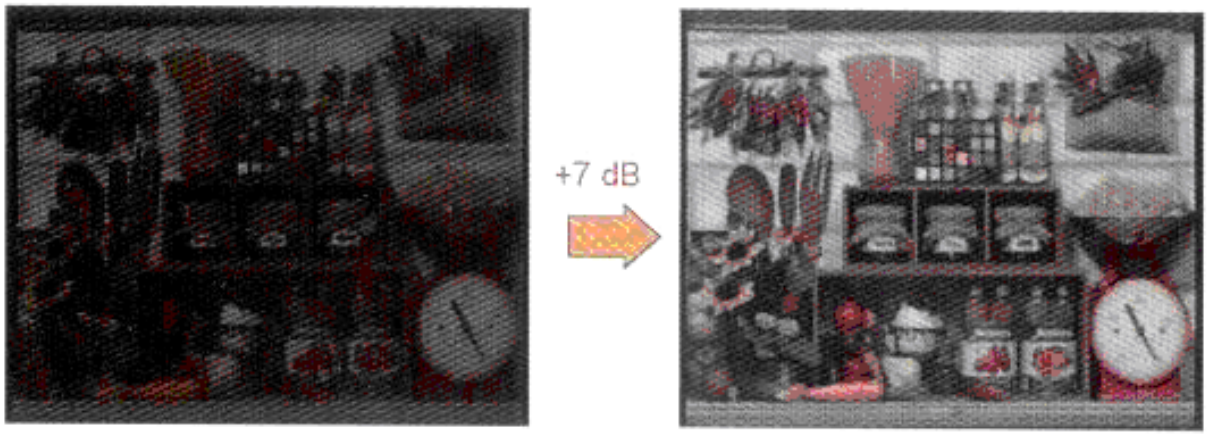


Рис.7. Сравнение чувствительности Super HAD CCD и Super HAD CCD II, у которой расширен динамический диапазон на 7 дБ

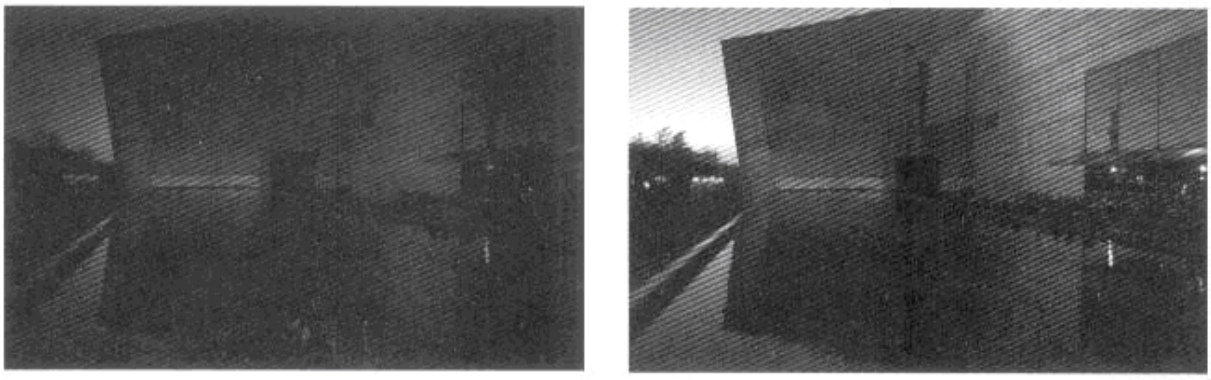


Рис. 8. Улучшение четкости изображения в условиях пониженной освещенности за счет применения функции цифрового подавления шумов

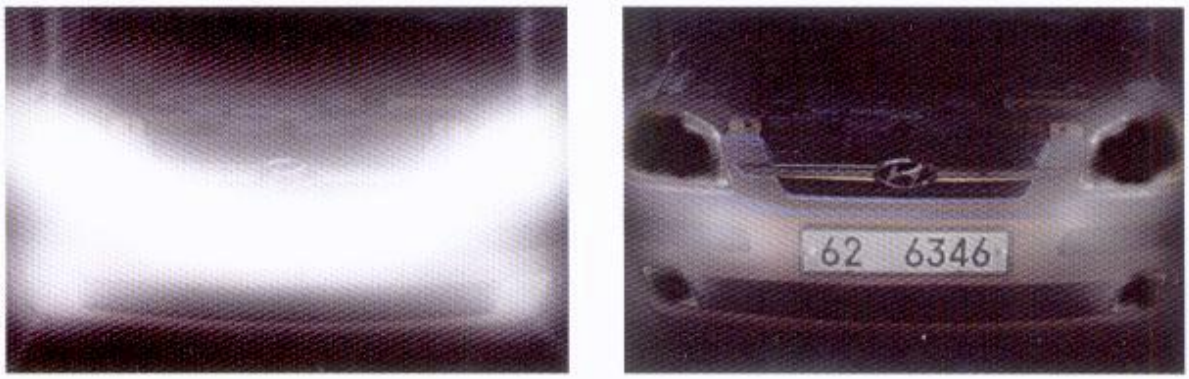


Рис. 9. Инверсия ярких засветок, позволяющая распознать номерной знак автомобиля с включенными фарами

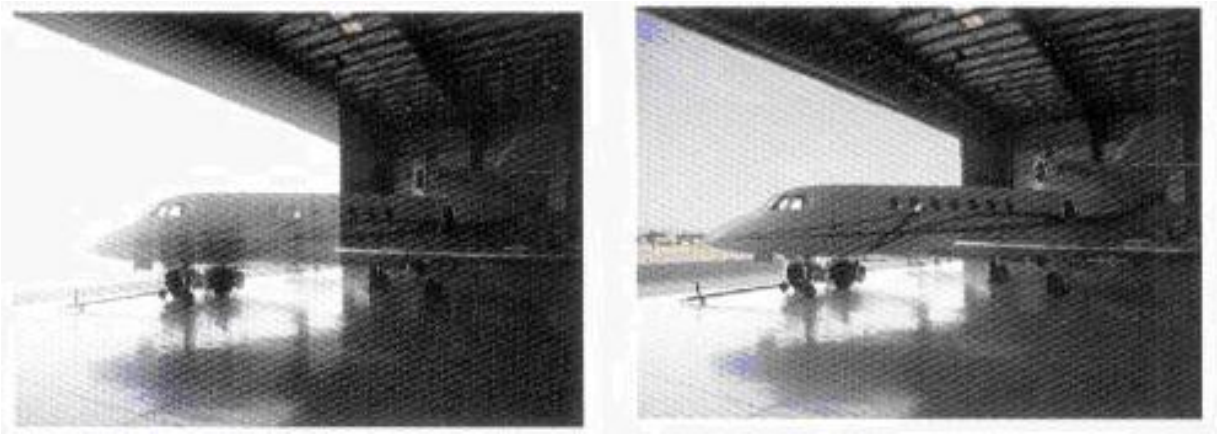


Рис. 10. Возможность одновременного наблюдения в зоне наблюдения как хорошо, так и плохо освещенных объектов за счет режима расширенного динамического диапазона

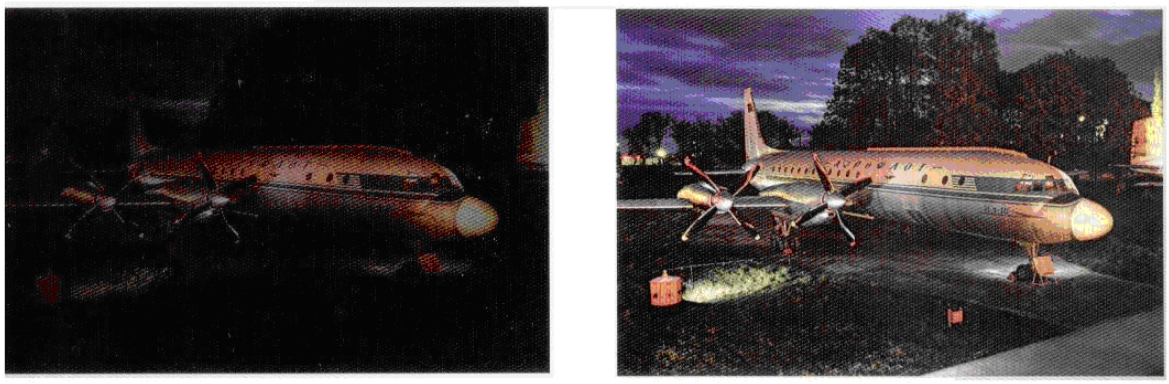


Рис. 11. Режим суммирования кадров
для повышения чувствительности ТВ камеры

Фирма ЭВС (РФ) [7-9] использует накопление заряда в матрице ПЗС от 0,02 с до 3 с (ТВ камеры фирмы Panasonic WV-BF550, WV-BL730), а также фирмы КАМРО (КС1003С) и РСАМ (РС-360D) с режимом «Electronic sensitivity enchanger». Однако при движении объекта наблюдения не происходит накопления заряда. В связи с этим такие ТВ камеры не нашли применения в системах безопасности.

Фирма ЭВС применяет метод «Technology EVS» В ТВ камерах VNC-542, VNC-742 это связано с суммированием зарядового изображения по площади непосредственно в матрице ПЗС. Суть метода в том, что дополнительное суммирование (накопление) сигнала производится в самой матрице ПЗС до того, как сигнал попал в выходное устройство и к нему присоединился шум считывания. В результате происходит сложение сигнала без сложения шума, а шум добавляется в выходном устройстве ПЗС один раз на каждую сумму сигналов. В результате 4-х кратное сложение приводит к 4-х кратному росту отношения сигнал/шум, а не к 2-х кратному, как для обычных методов. При уменьшении входной освещенности в ТВ камерах автоматически изменяется режим считывания сигнала с матрицы ПЗС – появляется суммарный сигнал: сначала сумма состоит из 2-х элементов, затем из 3-х, 4-х и т.д. до 10-12. В результате во столько же раз повышается чувствительность без смаза изображения. Но при низких уровнях освещенности происходит плавная потеря разрешения [7-9]. Такой режим возможен потому, что при малых сигналах шум считывания значительно превосходит фотонный шум, и последний практически не влияет на результат накопления.

В ТВ камерах фирмы ЭВС используется ночные режимы № 1 и № 2. Ночной режим № 1 заключается в автоматическом обмене разрешающей способности ТВ камеры на чувствительность при малых уровнях освещенности путем сложения сигналов с соседних пикселей. Максимальное число сложений равно 10 в ТВ камерах стандартного разрешения и 12 в ТВ камерах высокого разрешения. Это приводит с росту чувствительности в 10 и 12 раз соответственно. Ночной режим № 2 состоит в увеличении времени накопления

ТВ камеры при уменьшении освещенности до 16 ТВ кадров. Суммарный режим 1+2 позволяет в 100 раз повысить чувствительность [7-9].

Для большего увеличения чувствительности (до 4×10^{-5} лк) в ТВ камерах VNC-543 и VNC-743 используется сочетание режимов суммирования зарядового изображения по площади с режимом «Electronic sensitivity enchancer», но в ограниченном временном диапазоне (до 0,2 с), так, что смаз изображения движущихся объектов не очень высок. Чувствительность таких ТВ камер - как у приборов ночного видения с ЭОП поколений 2 и 2^{+}. На рис. 12 представлены типичные ТВ камеры фирмы ЭВС с повышенной чувствительностью, а в таблице 2 приложения – их основные параметры [7-9].

Для еще большего повышения чувствительности рекомендуется применение сверхсветосильных объективов с асферическими оптическими поверхностями и с относительным отверстием 1:0,8.

а. б. в.

г. д.

Рис. 12. Типичные ТВ камеры
с повышенной чувствительностью (Е) фирмы ЭВС:
а. – VNC-752-A3; б. – VNC-748-H2; в. – VNN-753-H3;
г. – VNI-752-H3; д. – VNI-553-A3

Следует отметить, что ТВ камеры фирмы ЭВС имеют ряд полезных особенностей: применение матриц ПЗС формата 1/3 и 1/2 дюймов с глобальным затвором обеспечивает минимальное искажение геометрии движущихся объектов по сравнению с применением КМОП матриц, работающих в режиме скроллинг-затвора; имеются два одновременно работающих выхода: цифровой (USB 2.0) и аналоговый (1 В, 75 Ом); диапазон возможных экспозиций составляет от 10 мкс до 24 мин, что обеспечивает наблюдение объектов при освещенности от 3×10^{5} до 2×10^{-6} лк; система тройного контрастирования

(вычитание уровня черного в предварительном и оконечном усилителях, а также в цифровой форме) обеспечивает возможность наблюдения объектов сквозь туман, дождь и снег в условиях, когда объекты становятся не видимыми человеческим глазом; высокая линейность видеотракта; автоматический электронный затвор с диапазоном экспозиций от 1/50 с до 1/100000 с; полное отсутствие смаза изображения от ярких объектов; адаптивный корректор четкости, адаптация к длине питающего кабеля; установка ТВ камер а автоматический режим, система автоматического определения типа объектива, уменьшение муаров и шумов за счет синхронного ввода цифрового сигнала «пиксель в пиксель»; питание ТВ камеры от USB интерфейса компьютера, встроенный корректор четкости и др. [7-9].

Повышения чувствительности ТВ камер за счет использования гибридно-модульных преобразователей изображения

Однако вместо режима накопления возможно создание гибридно-модульных преобразователей изображения (ГМП) [1]. В них экран электронно-оптического преобразователя (ЭОП) сопрягается с матрицей ПЗС. ЭОП преобразует изображение с низким уровнем освещенности в видимое и усиливает его по яркости. Поскольку ЭОП выполняет роль усилителя изображения – Image Intensifier (II) для ПЗС – Charge Coupled Device (CCD), то в зарубежной литературе ГМП сокращенно называют IICCD (Image Intensifier CCD).

При этом возможны два варианта построения ГМП [1]:

1. Матрица ПЗС находится вне ЭОП; изображение с экрана последнего с помощью оптики переноса (проекционный объектив или волоконно-оптическая деталь) передается на матрицу ПЗС. Она преобразует оптическое изображение в видеосигнал, который поступает в ТВ монитор для последующего наблюдения изображения с его экрана (собственно IICCD) (рис. 13а).
2. Матрица ПЗС располагается внутри ЭОП. На фотокатоде ЭОП создается изображение объекта и окружающего его фона. Фотокатод преобразует это изображение в электронное. Он усиливается электростатическим полем и переносится на матрицу ПЗС, смонтированную внутри ЭОП вместо экрана. При этом подложка матрицы ПЗС утончена до 10 – 15 мкм и обращена к потоку электронов. За рубежом такой ГМП называют Electron bombarded CCD (EBCCD) в отличие от традиционных IICCD, использующих внешнюю матрицу ПЗС.

На рис. 13а показаны ГМП IICCD фирмы ОАО «НПО Геофизика-НВ», на рис. 13б – ГМП IICCD фирмы Hamamatsu [1], а в таблице 3 приложения даны их основные параметры [10].

а. б.

Рис. 13. Типичные ГМП: а. – IICCD; б. – EBCCD

ГМП позволяют достигнуть чувствительности до 10^{-6} лк, причем без всякого накопления. ГМП могут работать в импульсном режиме, что позволяет их использовать в активно-импульсных приборах ночного видения (АИ ПНВ), обладающих всепогодностью, большой помехозащищенностью и высокой точностью измерения дальности до объекта наблюдения. Это позволяет эффективно работать по подвижным объектам. В ГМП EBCCD меньше масса и габариты, отсутствуют потери, связанные с преобразованием электронного потока в излучение экрана ЭОП, энергетические потери в оптике переноса, потери разрешающей способности и контраста в этой оптике, отсутствует влияние инерционности ЭОП и его шумы из-за отсутствия самого ЭОП. На рис. 14 показано преимущество EBCCD по сравнению с ICCD.

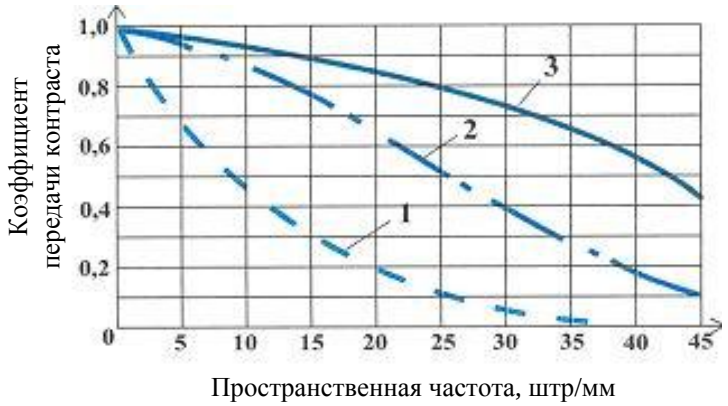


Рис. 14. Типичные кривые передачи контраста для:
традиционных ICCD (кривая 1), EBCCD (кривая 2) и матрицы ПЗС (кривая 3)

Фирма Hamamatsu (Япония) разработала EBCCD – модели N7220-61, N76461, N7640-64 [1]. Первые две модели используют фотокатод GaAs, работающий в области спектра 0,37-0,92 мкм, а третья модель – фотокатод GaAsP, работающий в области спектра 0,28-0,72 мкм. Модель N7220-61 имеет размер чувствительной площадки фотокатода 12,2×12,2 мм, число пикселей 512×512, усиление 1300 (при напряжении 8 кВ), а две другие модели – соответственно размер 9,2×6,8 мм, число пикселей 658×494, а усиление 700 (при напряжении 6 кВ) и 200 (при напряжении 2 кВ) (рис. 13б). Но EBCCD не

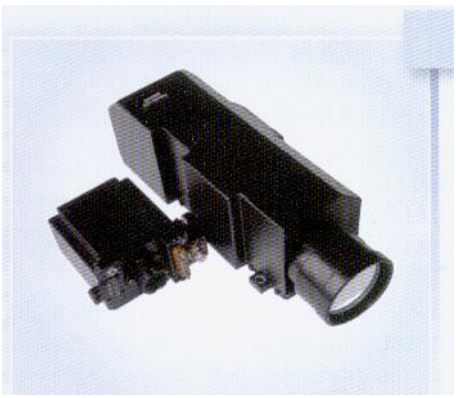
получили широкого распространения из-за технологической сложности и высокой стоимости изготовления.

В таблицах 4, 5 в приложении представлены параметры типичных ТВ систем на основе ГМП [10, 11].

На рис. 15 показаны типичные ТВ камеры на основе ГМП.

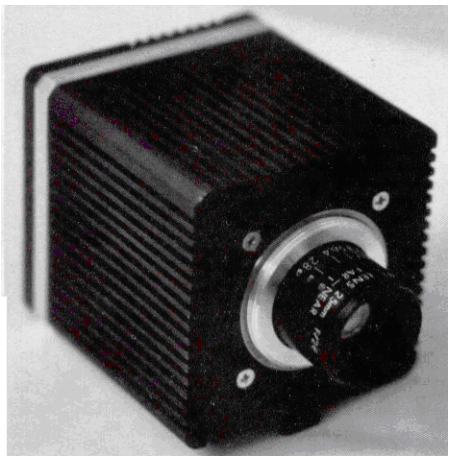
Преимущество матрицы ПЗС связано также с возможностью получить при определенном уровне пониженной освещенности цветное изображение. ТВ камера на основе ПЗС может выполнять роль насадки для дневных приборов наблюдения и прицеливания, а также для приборов ночного видения (ПНВ) на базе ЭОП с целью вывода их изображений в видеомагнитофон, в персональный компьютер, в карманный персональный компьютер, в смартфон. Это особенно важно для криминалистики и работы спецслужб. Изображения можно запомнить, тиражировать их, обрабатывать в реальном масштабе времени, передавать их дистанционно, микшировать с изображениями, создаваемыми другими каналами (в частности, тепловизионным каналом). Таким образом, отказ от ГМП является насущной необходимостью, даже не взирая на его высокую чувствительность.

а.



б.

в.



г.

Рис.15. Типичные ТВ камеры на основе ГМП:
а. – ГЕО-ПЗР-1; б. - ГЕО-НТК 4; в. – ГЕО-УФ; г. – «Кречет»

Повышение чувствительности ТВ камер благодаря использованию матриц ПЗС с электронным умножением

Реальная возможность для этого представилась с появлением матриц ПЗС с электронным умножением – Electron Magnification CCD (EMCCD) [12-19]. Лидером в создании EMCCD является компания e2V (Великобритания). Эта компания была создана в 1947 г. под названием Phoenix Dynamo и в этом же году переименована в English Electric Company, с 1999 г. по 2002 г. – Marcony Applied Technologies, с 2002 г. – e2V. Компания разработала и производит EMCCD под товарным знаком L3Vision. Кроме фирмы e2V, EMCCD производят также фирмы Ander Technology (Великобритания) и Hamamatsu Photonics Япония) [10].

Сигнал изображения, представляющий собой электрический заряд, усиливается непосредственно на кристалле. Это позволяет матрице ПЗС работать в реальном масштабе времени с шумом считывания в 1 электрон. Матрица ПЗС благодаря этому регистрирует единичные фотоны. Главная особенность всех традиционных матриц ПЗС, препятствующая получение изображения низкоуровневых сигналов, является фотонный шум считывания, ограничивающий требуемое отношение сигнал/шум. Главная особенность EMCCD – возможность умножения возникающего заряда, т.е. повышение уровня сигнала еще до процесса считывания зарядовых пакетов. Это снижает уровень шума считывания до второстепенного его значения и позволяет повысить отношение сигнал/шум при низких уровнях освещенности. На рис. 16 показана структурная схема EMCCD.

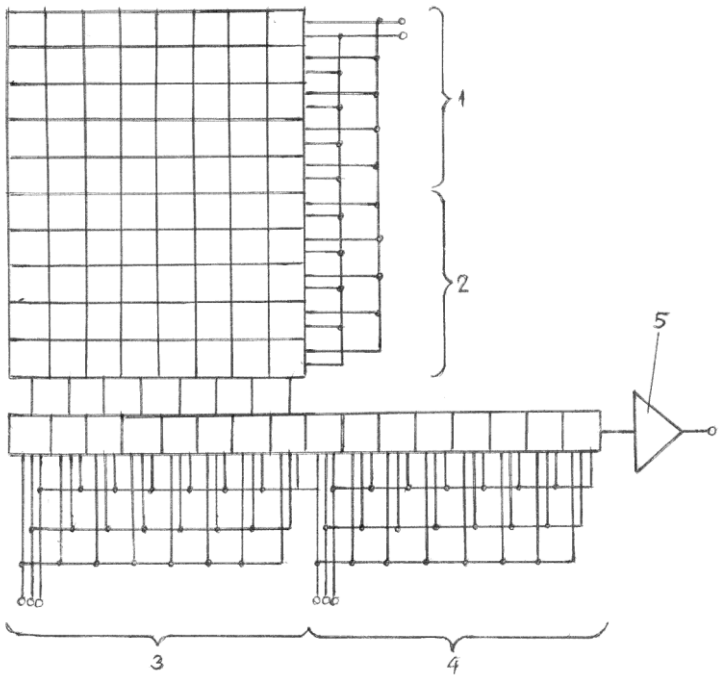


Рис. 16. Структурная схема EMCCD:
1 – секция экспонирования; 2 – секция хранения;
3 – регистр считывания; 4 – регистр умножения;
5 – преобразователь заряд-напряжение

По сравнению с традиционной схемы матрицы ПЗС с кадровым переносом в структурной схеме EMCCD имеется дополнительный регистр умножения. По своей структуре он близок к регистру считывания, но использует систему электродов с более высоким напряжением тактирующих импульсов. Повышенное напряжение позволяет инициировать лавинный пробой. Благодаря этому происходит умножение считываемого заряда. Лавинное умножение происходит при переходе заряда из ячейки в ячейку. При каждом таком переходе в результате лавинного умножения исходный заряд увеличивается незначительно – на 1,5-2%, но после прохождения нескольких сотен ячеек регистра умножения результирующий коэффициент усиления может достигать 100-1000. При низких значениях коэффициента лавинного умножения процесс электронного усиления является мало шумящим. Это позволяет увеличивать сигнальный заряд при практически неизменном шуме на выходе матрицы. Если пиксель матрицы ПЗС регистрирует отдельный фотон, то на вход преобразователя заряд-напряжение поступает сигнальный заряд с числом 100 электронов, по сравнению с которым шум считывания не играет существенной роли. Это и позволяет поднять отношение сигнал/шум. В матрице EMCCD используется обратное ее освещение (рис. 17).

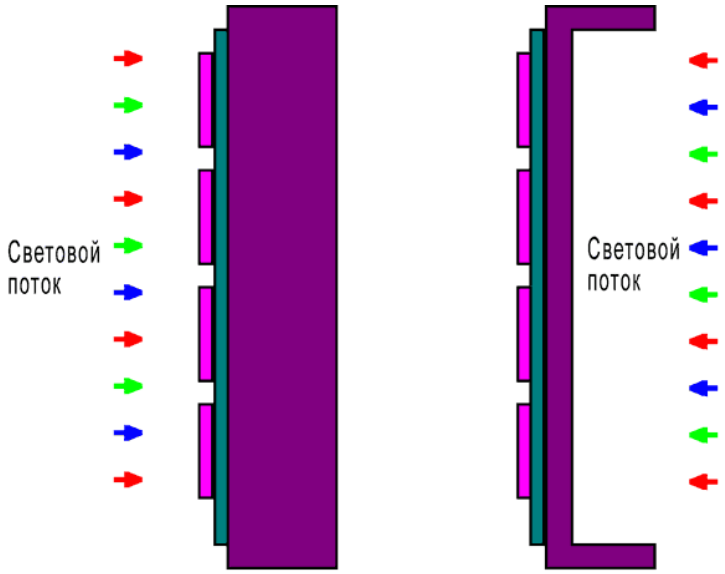


Рис. 17. Прямое и обратное освещение матрицы ПЗС

Это устраняет потери, обусловленные прохождением излучения через электроды, которые характерны для прямой засветке матрицы ПЗС. Благодаря этому квантовая эффективность EMCCD приближается к теоретическому пределу. Возможность изменения толщины поглощающего слоя при обратном освещении в сочетании с просветляющими покрытиями позволяет также оптимизировать спектральную кривую квантового выхода EMCCD.

Типичные кривые зависимости квантовой эффективности EMCCD от длины волны представлены на рис. 18.

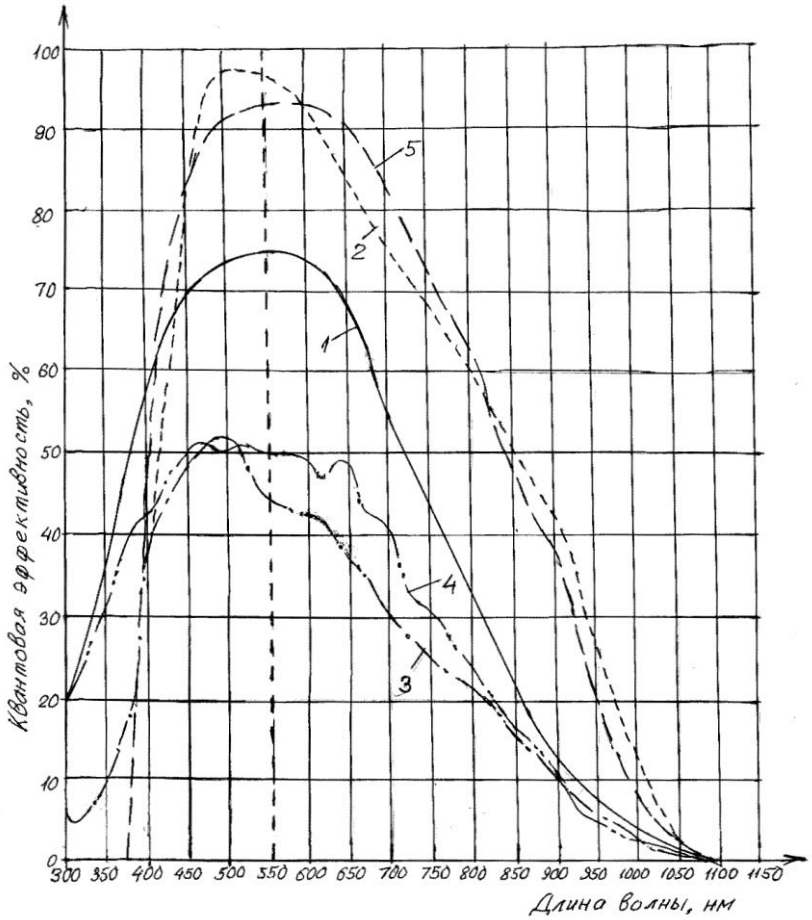


Рис. 18. Типичные кривые зависимости квантовой эффективности EMCCD от длины волны (штриховой прямой на графике показана длина волны, соответствующей квантовой эффективности 93%): а – Hawk 828/829; б – Hawk EM216; в – Hawk EM247; г – EMCCD матрицы TS246CYM-BO, д – паспортная кривая квантовой эффективности матрицы EMCCD 97

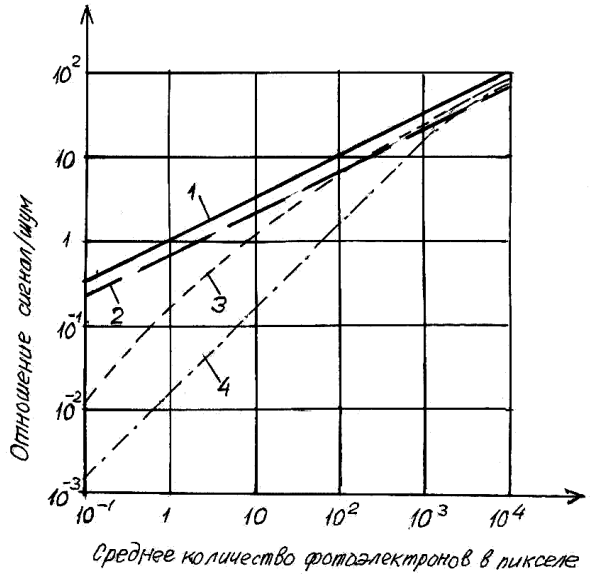


Рис.19. Отношение сигнал/шум в EMCCD как функция среднего числа фотоэлектронов в зарядовом пакете: кривая 1 – теоретический предел; кривые при температуре: 2 – (-40)°C, 3 – (-20)°C, 4 – без умножения при (+20)°C

Помимо снижаемого здесь шума считывания, есть и другие составляющие шума. Для подавления шума термоэмиссии применяется охлаждение EMCCD. Из графика рис. 19 видно, что при охлаждении EMCCD до (-40)°C отношение сигнал/шум приближается к теоретическому пределу.

Это позволяет регистрировать субфотонные изображения. Наведенный в EMCCD шумовой заряд, зависящий от количества переносов сигнальных зарядов из ячейки в ячейку, при тщательном подборе формы управляющих импульсов переноса составляет незначительную величину – менее 10^{-6} электрона на каждый перенос.

Рис. 20. Возможности EMCCD по сравнению с другими описанными выше устройствами с точки зрения работы при пониженных уровнях освещенности.

Уровни освещенности:

- Daylight – дневной свет;
- Overcast & Twilight – облачность и сумерки;
- Full moon – ночь, полная луна;
- Quarter moon – ночь, четверть луны;
- Moon less (Starlight) – безлунная ночь (звездный свет);
- Moon less (Overcast) – безлунная облачная ночь.

Устройства:

- Conventional CCTV – ТВ камеры на основе традиционных матриц ПЗС;
- Low Light CCD – ТВ камеры на основе матриц ПЗС, чувствительных к низким уровням освещенности;
- Gen II Intensifier tube – приборы на базе ЭОП 2-го поколения;
- Gen III Intensifier tube – приборы на основе ЭОП 3-го поколения;
- Raptor's EMCCD Technology – EMCCD фирмы Raptor

В EMCCD вместо механического затвора используется жидкокристаллический затвор. Это позволяет осуществить процесс считывания в матрице ПЗС без влияния вибраций. 16-биный выход USB 2 позволяет

осуществить быстрое подключение EMCCD к персональному компьютеру и высококачественное воспроизведение изображения.

Недостатком EMCCD является их пока еще высокая стоимость – на порядок выше, чем у традиционных матриц ПЗС. Однако есть возможности ее снижения в будущем.

На рис. 20 наглядно представлены повышенные возможности EMCCD по сравнению с другими описанными выше устройствами с точки зрения работы при пониженных уровнях освещенности.

На рис. 21 показано, что дает повышенная чувствительность ТВ камер на основе EMCCD по сравнению с ТВ камерами на основе традиционных ПЗС.

На рис. 22 показано преимущество ТВ камер на основе EMCCD с точки зрения расширения зоны охвата и их преимущество при ночном наблюдении.

Рис. 21. Возможности ТВ камер на основе EMCCD по сравнению с ТВ камерами на основе традиционных ПЗС с точки зрения чувствительности

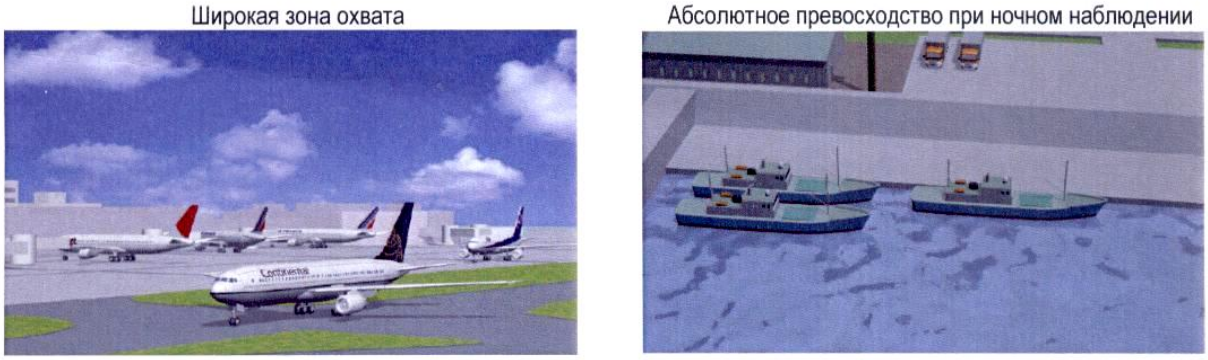


Рис. 22. Преимущества ТВ камер на основе EMCCD с точки зрения расширения зоны охвата и преимущества при ночном наблюдении

На рис. 23 представлены типичные ТВ камеры на основе EMCCD. Представленные на рис. 23б три ТВ камеры на основе матрицы ПЗС EM CCD и ТВ камеры KP-DE500 различаются по увеличению: модель HC-268 имеет переменное увеличение 16^x zoom, HC-278 – 30^x zoom, HC-278-H6 – 55^x zoom.

Основные параметры матриц ПЗС EMCCD представлены в таблице 6 приложения, а ТВ камер на их основе – в таблице 7, там же.

Анализ данных, представленных в таблицах, показывает несомненные преимущества EMCCD и ТВ камер на их основе по сравнению с соответствующими устройствами на основе обычных матриц ПЗС.

Рис. 23. Типичные ТВ камеры на основе EMCCD:
а – KP-DE500; б – три модели ТВ камер на основе матриц ПЗС EMCCD;
в – S4X; г – SC200PK; д – Synapse EM; е – 360-229 Falcon-EMCCD;
ж – Hawk 247-CL, Hawk 216-A; з – три ТВ камеры ev2v L3 Vision

Заключение

Проведенный выше анализ показывает, что существуют реальные возможности создания и применения в системах безопасности высокочувствительных ТВ камер различного типа. При этом можно уверенно рассчитывать на высокую перспективность EMCCD и ТВ камер на их основе для применения в указанных системах и в специальной технике.

Приложение

Таблица 1 – Сравнительные параметры высокочувствительных ТВ камер фирмы Watec (Япония)

№ п/п	Модель	Формат, дюйм	Разрешение, ТВ линий	Рабочая освещенность, лк	Относительно отверстие объектива	Напряжение питания, В	Ток потребления, мА	Габариты, мм
1	WAT-902H	1/2	570	$3x10^{-4}$	1:1,2	12	160	36x36x58
2	WAT-502B	1/3	400	$3x10^{-3}$	1:1,4	9 (7 – 11)	130	30x30x46
3	WAT-107L	1/3	420	$5x10^{-3}$	1:1,4	24	160	44x44x45
4	WAT-525EX	1/2	550	$2x10^{-3}$	1:1,4	12		44x44x53
5	WAT-902B	1/2	570	$3x10^{-3}$	1:1,4	12	135	34x34x58
6	LCL-902K	1/2	>570	$1,5x10^{-4}$	1:1,2	12	180	34x37x52
7	LCL-902Q	1/2	>570	10^{-2}	1:1,2	12	180	29x29x50
8	LCL-903K	1/3	>500	$3x10^{-4}$	1:1,2	12	180	34x37x65
9	LCL-903Q	1/3	500	$3x10^{-4}$	1:1,2	12	180	29x29x50
10	LCL-811K	1/3	400	10^{-4}	1:1,4	12	180	34x37x52
11	LCL-196	1/3	480 (ЦВ) >570 (ЧБ)	$9x10^{-2}$ (ЦВ) $9x10^{-3}$ (ЧБ)	1:1,2 (ЦВ) 1:1,2 (ЧБ)	12		43x43x60

Примечания: отношение сигнал/шум 46 – 50 дБ, экспозиция электронного затвора 1/50 – 1/100 000 с, гамма-коррекция 0,45-1, диапазон рабочих температур (-10) – (+40)°С.

Таблица 2 – Сравнительные параметры высокочувствительных ТВ камер фирмы ЭВС (Россия)

№ п/п	Модель	Формат, дюймы	Число пикселей	Разрешение, ТВ линий	Рабочая освещенность, лк	Относительное отверстие объектива	Напряжение питания, В	Ток потребления, мА	Отношение сигнал/шум, дБ	Габариты, мм	Максимальный коэффициент бининга	Максимальный коэффициент суммирования полей	Режим увеличения чувствительности, крат	Примечание
1	VSA-531	1/3	500x582	380	$5x10^{-3}$	1:1,2	9-15	115	48	42x42x24				EXview HAD CCD Авт. определ. объектива (DD, VD, manual)
2	VSA-786	1/2	752x582	570	$5x10^{-3}$	1:1,2	9-15	140	52	42x42x28				EXview HAD CCD
3	VNA-542-A3	1/3	500x582	380	$1,5x10^{-3}$ $5x10^{-4}$	1:2 1:0,8	9-13,5	130	48	42x42x25	7x2		10	EXview HAD CCD
4	VNA-543-A3	1/3	500x582	380	$1,2x10^{-4}$ $2x10^{-5}$	1:2 1:0,8	9-13,5	160	48	42x42x40	7x2	16	100	EXview HAD CCD
5	VNA-742-A3	1/3	752x582	570	$3x10^{-3}$ $5x10^{-4}$	1:2 1:0,8	9-13,5	130	48	42x42x24	7x2		10	EXview HAD CCD
6	VNA-742-H3	1/3	752x782	570	$1,5x10^{-3}$ $4x10^{-4}$	1:2 1:0,8	9-13,5	130	48	42x42x24	7x2		10	EXview HAD CCD
7	VNA-743-A3	1/3	752x582	570	$1,5x10^{-4}$ $4x10^{-5}$	1:2 1:0,8	9-13,5	160	48	42x42x40	7x2	16	100	EXview HAD CCD
8	VNA-743-H3	1/3	752x582	570	10^{-4} $2x10^{-5}$	1:2 1:0,8	9-13,5	160	48	42x42x40	7x4	18	100	New generation EXview HAD CCD
9	VNI-743-H2	1/2	752x582	570	$4x10^{-5}$	1:0,8	9-13,5	160	52	42x42x35	7x2	18	100	EXview HAD CCD
10	VNA-748-H3	1/3	752x582	570	$5x10^{-3}$ $5x10^{-5}$	1:2 1:0,8	9-15	110	48	42x42x39	8x4	256 (4096-ручной режим)	100	New generation EXview HAD CCD
11	VNI-748-H2	1/2	752x582	570	$5x10^{-5}$	1:0,8	9-15	110	52	42x42x39	8x4	256 (4096-ручной режим)	100	EXview HAD CCD

№ п/п	Модель	Формат, дюймы	Число пикселей	Разрешение, ТВ линий	Рабочая освещенность, лк	Относительное отверстие объектива	Напряжение питания, В	Ток потребления, мА	Отношение сигнал/шум, дБ	Габариты, мм	Максимальный коэффициент бининга	Максимальный коэффициент суммирования полей	Режим увеличения чувствительности, крат	Примечание
12	VNS-742-A3	1/3	752x582	570	$3x10^{-3}$	1:2	9-13,5	130	48	Ø118x75 (купол)	7x2		10	EXview HAD CCD
13	VNS-742-H3	1/3	752x582	570	$1,5x10^{-3}$	1:2	9-13,5	130	48	Ø118x75 (купол)	7x2		10	New generation EXview HAD CCD
14	VSC-541	1/3	500x582	380	$5x10^{-3}$	1:1,2	9-15	75	48	56x50x92				EXview HAD CCD
15	VSC-746	1/2	752x582	570	$5x10^{-3}$	1:1,2	9-15	90	52	56x50x92				EXview HAD CCD
16	VNC-542-A3	1/3	500x582	380	$5x10^{-4}$	1:0,8	9-13,5	130	48	56x50x92	7x2		10	EXview HAD CCD
17	VNC-543-A3	1/3	500x582	380	$2x10^{-5}$	1:0,8	9-13,5	160	48	56x50x92	7x2	16	100	EXview HAD CCD
18	VNC-742-A3	1/3	752x582	570	$5x10^{-4}$	1:0,8	9-13,5	130	48	56x50x92	7x2		10	EXview HAD CCD
19	VNC-724-H3	1/3	752x582	570	$4x10^{-4}$	1:0,8	9-13,5	130	48	56x50x92	7x2		10	New generation EXview HAD CCD
20	VNC-743-A3	1/3	752x582	570	$4x10^{-5}$	1:0,8	9-13,5	160	48	56x50x92	7x2	16	100	EXview HAD CCD
21	VNC-743-H3	1/3	752x582	570	$2x10^{-5}$	1:0,8	9-13,5	160	48	56x50x92	7x4	18	100	New generation EXview HAD CCD
22	VNC-743-H2	1/2	752x582	570	$4x10^{-5}$	1:0,8	9-13,5	160	52	56x50x92	7x2	18	100	EXview HAD CCD
23	VNC-748-H3	1/3	752x582	570	$5x10^{-5}$	1:0,8	9-13,5	160	48	56x50x92	8x4	256 (4096 – ручной режим)	100	New generation EXview HAD CCD
24	VNC-748-H2	1/2	752x582	570	$3x10^{-4}$	1:0,8	9-14	110	52	50x57x93	8x4	256 (4096 – ручной режим)	100	EXview HAD CCD, Масса 220 г, частота кадров 25 Гц
25	VNP-542-A3	1/3	500x782	380	$1,5x10^{-3}$	1:2	9-13,5	130	48	125x95x235	7x2		10	EXview HAD CCD
26	VNP-742-A3	1/3	752x582	570	$3x10^{-3}$	1:2	9-13,5	210	48	125x95x235	7x2		10	EXview HAD CCD
27	VNP-742-H3	1/3	752x582	570	$1,5x10^{-3}$	1:2	9-13,5	210	48	125x95x235	7x2		10	New generation EXview HAD CCD
28	VSN-541	1/3	500x582	380	$5x10^{-3}$	1:1,2	9-13,5	250	48	140x120x190				EXview HAD CCD
29	VSN-746	1/2	752x582	570	$5x10^{-3}$	1:1,2	9-13,5	280	52	140x120x190				EXview HAD CCD
30	VNN-542-A3	1/3	500x582	380	$5x10^{-4}$	1:0,8	9-13,5	300	48	140x120x190	7x2		10	EXview HAD CCD
31	VNN-543-A3	1/3	500x582	380	$2x10^{-5}$	1:0,8	9-13,5	320	48	140x120x190	7x2	16	100	EXview HAD CCD
32	VNN-742-A3	1/3	752x582	570	$5x10^{-4}$	1:0,8	9-13,5	300	48	140x120x190	7x2		10	EXview HAD CCD
33	VNN-742-H2	1/3	752x582	570	$4x10^{-4}$	1:0,8	9-13,5	300	48	140x120x190	7x2		10	New generation EXview HAD CCD
34	VNN-743-A3	1/3	752x582	570	$4x10^{-5}$	1:0,8	9-13,5	320	48	140x120x190	7x2	16	100	EXview HAD CCD
35	VNN-743-H3	1/3	752x582	570	$2x10^{-5}$	1:0,8	9-13,5	320	48	140x120x190	7x4	18	100	New generation EXview HAD CCD
36	VNN-743-H2	1/2	752x582	570	$4x10^{-5}$	1:0,8	9-13,5	320	52	140x120x190	7x2	18	100	EXview HAD CCD
37	VMC-745-H3	1/3	752x582	460	$5x10^{-3}$	1:0,8	8-16	160	48	56x50x92			10	DSP, New generation EXview HAD CCD, режим супер «день/ночь»
38	VMN-745-H3	1/3	752x582	460	$5x10^{-3}$	1:0,8	8-16	300	48	140x120x190			10	DSP, New generation EXview HAD CCD, режим супер «день/ночь»
39	VBC-541-USB	1/3	500x576	380	$1,5x10^{-2}$ (1) $3x10^{-5}$ (2) $6x10^{-6}$ (3)	1:1,2		250	52	56x50x92				

№ п/п	Модель	Формат, дюймы	Число пикселей	Разрешение, ТВ линий	Рабочая освещенность, лк	Относительное отверстие объектива	Напряжение питания, В	Ток потребления, мА	Отношение сигнал/шум, дБ	Габариты, мм	Максимальный коэффициент бининга	Максимальный коэффициент суммирования полей	Режим увеличения чувствительности, крат	Примечание
40	VSC-541-USB	1/3	500x576	380	$5x10^{-3}$ (1) $1x10^{-5}$ (2) $2x10^{-6}$ (3)	1:1,2		250	52	56x50x92				
41	VBC-741-USB	1/3	752x576	580	$2x10^{-2}$ (1) $4x10^{-5}$ (2) $8x10^{-6}$ (3)	1:1,2		280	48	56x50x92				
42	VSC-741-USB	1/3	752x576	580	$2x10^{-2}$ (1) $4x10^{-5}$ (2) $8x10^{-6}$ (3)	1:1,2		280	48	56x50x92				
43	VSC-746-USB	1/2	752x576	580	$5x10^{-3}$ (1) $1x10^{-5}$ (2) $2x10^{-6}$ (3)	1:1,2		300	52	56x50x92				
44	VNC-752-A3	1/3		570	$6x10^{-4}$		9-14	130		50x57x63				Масса 120 г, частота кадров 25 Гц
45	VNN-752-H2	1/2		570	$2x10^{-5}$		9-14	120		50x57x63				Масса 220 г, частота кадров 25 Гц
46	VNN-753-H3	1/3		570	$3x10^{-5}$		9-14			140x183x325				Масса 1300 г, частота кадров 25 Гц, диапазон рабочих температур (-50)-(+50)°С, 1+2 ночной режим, наружная ТВ камера
47	VSC-551-USB	1/3		380	$5x10^{-3}$ (ручной режим) 10^{-5} (автомат. режим, экспозиция 10 с), $2x10^{-6}$ (автомат. режим, экспозиция 2 мин, охл.)		5	250		50x57x93				Масса 150 г, частота кадров 25 Гц
48	VSC-751-USB	1/3		570	$1,2x10^{-2}$ (ручной режим) $3x10^{-5}$ (автомат. режим, экспозиция 10 с), $6x10^{-6}$ (автомат. режим, экспозиция 2 мин, охл.)		5	280		50ч57x93				Масса 150 г, частота кадров 25 Гц

№ п/п	Модель	Формат, дюймы	Число пикселей	Разрешение, ТВ линий	Рабочая освещенность, лк	Относительное отверстие объектива	Напряжение питания, В	Ток потребления, мА	Отношение сигнал/шум, дБ	Габариты, мм	Максимальный коэффициент бининга	Максимальный коэффициент суммирования полей	Режим увеличения чувствительности, крат	Примечание
49	VSC-756-USB	1/2		570	$5x10^{-3}$ (ручной режим) 10^{-5} (автомат. режим, экспозиция 10 с), $2x10^{-6}$ (автомат. режим, экспозиция 2 мин, охл.)		5	300		50x57x93				Масса 150 г, частота кадров 25 Гц
50	VNI-553-A3	1/3		380	$4x10^{-5}$		9-14	120		42x42x55				Масса 50 г, частота кадров 25 Гц, бескорпусной
51	VNI-752-H3 (VNI-752-H3-VS)	1/3		570	$4x10^{-4}$		9	100		42x42x24				Масса 30 г, частота кадров 25 Гц, бескорпусной
52	VMC-750-HR			540	$5x10^{-3}$ (цветной режим), $3x10^{-3}$ (ч/б режим), $2x10^{-4}$ (ч/б режим с повышенной чувствительностью		9-14	90		50x57x63				Масса 100 г, частота кадров 25 Гц
53	VMN-750-HR			540	$5x10^{-3}$ (цветной режим), $3x10^{-3}$ (ч/б режим), $2x10^{-4}$ (ч/б режим с повышенной чувствительностью		9-14	250		140x185x325				Масса 1300 г, частота кадров 25 Гц, наружная ТВ камера

Примечания: указанные в таблице рабочие освещенности приведены для отношения сигнал/шум 10 дБ, а для позиций 39 – 43 – 20 дБ, (1) – в автоматическом режиме, (2) – при экспозиции 10 с, (3) – при экспозиции 2 минуты (0°C).

Таблица 3 – Основные параметры ГМП ОАО «НПО Геофизика-НВ»

№ п/п	Наименование параметра	Модель ГМП			
		ФПМ В-ИК	ФПМ УФ	ФПМ ИК1	ФПМ ИК2
1	Рабочая область спектра, мкм	0,5 – 0,9	0,25 - 0,35	0,4 – 1,1	0,95 – 1,65
2	Интегральная чувствительность, мкА/лм	2500		400	
3	Спектральная чувствительность на длине волны 0,85 мкм, мА/Вт	220		50	
4	Спектральная чувствительность на длине волны 1,06 мкм, мА/Вт			2,5	
5	Разрешение, ТВ линий	450	400	400	450
6	Отношение сигнал/шум	20		9	
7	Рабочая освещенность, Вт/м^2		$5x10^{-4}$		
8	Пороговая освещенность, Вт/м^2		$5x10^{-7}$		
9	Квантовый выход на длине волны 1,54 мкм, %				2

Примечания: для всех ГМП формат изображения 768x576 пикселей, разрядность выходного сигнала 12 бит, напряжение питания = 12 В, ток потребления 250 мА.

Таблица 4 – Основные параметры высокочувствительных ТВ камер на основе ГМП

№ п/п	Фирма	Модель	Состав	Рабочая освещенность, лк	Дальность действия	Угол поля зрения, град.	Разрешение, ТВ линий	Масса, кг	Габариты, м	Напряжение питания, В/Энергопотребление, Вт	Диапазон рабочих температур, °С	Примечание
1	ОАО «НПО Геофизика-НВ»	ГЕО-ПЗР1	НТВС, ДТВ	$(3-5)x10^{-3}$ - 1	Не менее 10 км по вертолету типа МИ-8	8x6° или 24,7x18,5°	350-400	Не более 15	ТВ камеры: 400x270x120 ТВ монитора: 180x220x50	=27/13,5	(-40) – (+50)	ТВ наблюдательный прибор для обнаружения, сопровождения и применения управляемых ракет модернизированного комплекса «Стрела-10М». ТВ стандарт -625 линий, частота кадров 50 Гц
2	ОАО «НПО Геофизика-НВ»	ГЕО-НТК3	НТВС, ДТВ	$5x10^{-3}$ - 10	1,5-2 км по бронетанковой технике	10,6x8°	350-400	Блок оптико-электронный: 2,2 Блок электронный: 0,8	Блок оптико-электронный: 200x112x190 Блок электронный: 156x148x105	=27/13,5	(-40) – (+50)	Ночная визирная система для вертолетов Ми-8МВ. Для ДТВ матрица ПЗС с числом пикселей 752x582, рабочая освещенность 0,5 – 150 лк ТВ стандарт -625 линий, частота кадров 50 Гц
3	ОАО «НПО Геофизика-НВ»	ГЕО-НТК4	НТВС, ДТВ	$5x10^{-3}$ – $5x10^{4}$	1,5-2 км по бронетанковой технике	Днем: 13,5x18° Ночью: 11x8,4°	Днем: 500 Ночью: 350-400	НТВС: 1,7 ДТВ: 0,7	НТВС: 225x87x90 ДТВ: 117x53x91	=12/6	(-40) – (+50)	Круглосуточная ТВ система для обзорных стабилизированных систем вертолетов. Для ДТВ матрица ПЗС с числом пикселей 752x582, рабочая освещенность 0,5 – 150 лк ТВ стандарт -625 линий, частота кадров 50 Гц

№ п/п	Фирма	Модель	Состав	Рабочая освещенность, лк	Дальность действия	Угол поля зрения, град.	Разрешение, ТВ линий	Масса, кг	Габариты, м	Напряжение питания, В/Энергопотребление, Вт	Диапазон рабочих температур, °С	Примечание
4	ОАО «НПО Геофизика-НВ»	ГЕО-НТК5	НТВС, ДТВ		По автотранспортной технике днем 4 км, ночью 3 км	10,6x8°	Днем: 500 Ночью: 350-400	Платформы: 9 Электронного модуля: 24	Платформы: Ø300x320 Электронного модуля: Ø300x350x200	=27/13,5	(-40) – (+50)	Круглосуточная стабилизированная ТВ система для вертолетов. Для ДТВ матрица ПЗС с числом пикселей 752x582, рабочая освещенность 0,5 – 150 лк ТВ стандарт -625 линий, частота кадров 50 Гц
5	ОАО «НПО Геофизика-НВ»	Круглосуточная АИ ТВ камера с повышенной дальностью действия АИ ТВ-ГЕО	НТВС, ДТВ	10^{-4} – $5x10^{4}$	По группе людей 1 – 2 км	Днем: 1,1x1,5° Ночью: 2x3°	Днем: 570 Ночью: 450	11	1350x310x230	=12/-	(-40) – (+40)	Предварительное обнаружение объектов наблюдения достигается с применением канала поиска на основе РЛС или тепловизионного канала
6	ОАО «НПО Геофизика-НВ»	Высокочувствительная ТВ камера для УФ области спектра ГЕО-УФ	НТВС	Круглосуточно; $E_{рабоч.} = 5x10^{-4}$ Вт/м^2 $E_{порог.} = 5x10^{-7}$ Вт/м^2			450	0,8	75x75x80	=12/6		Матрица ПЗС с числом пикселей 752x582, размер пикселя 22x22 мкм, чувствительная поверхность 11,3x11,3 мм, ЭОП 3-го поколения с фотокатодом GaN
7	ОАО «НПО Растр»	КП-181	НТВС	10^{-3} - 10		32,7x24,9° 20,9x15,8° 14,6x11°	350	3	353x143x102	=12 или ~ 220 В 50 Гц/-	(-40) – (+45)	
8	ОАО ЦНИИ «Циклон»	Циклон-DN/CCD-1,2	НТВС, ДТВ	10^{-4} – 10^{-3}	Обнаружение/ распознавание: человека: 6,5/3 км автомашины: 14/6 км	ДТВ: 0,9x0,7° НТВС: 2,4x1,8 и 1,2x0,9°°	45 штр/мм	38	820x310x240	=24 или ~ 220 В 50 Гц/-		
9	ОАО ЦНИИ «Циклон»	Кречет	НТВС	Круглосуточно	Обнаружение/ распознавание: автомашины: 10/4,5 км	40x24° 30x18°	40 штр/мм	8	120x200x450	=12, =24 или ~ 220 В 50 Гц/70		

Примечания: НТВС – низкоуровневая ТВ система, ДТВ – дневной ТВ канал.

Таблица 5 – Некоторые параметры ТВ камер на основе ГМП различных фирм [20]

№ п/п	Страна	Фирма	Модель	Чувствительность, лк	Разрешение, ТВ линий	Поколение ЭОП
1	Япония	Panasonic	WV-BD900	$1,5x10^{-3}$	420	2
2	Россия	TURN	LINX120	10^{-4}	350	2^{+}
3	Германия	JAI	JAI-757	$5x10^{-3}$	510	2^{++}
4	Германия	JAI	JAI-757A	10^{-4}	450	3

Примечание: т.к. для ТВ камер с ГМП чувствительность приводится обычно для изображения хорошего качества, то при полном разрешении, т.е. при отношении сигнал/шум 34 -36 дБ, для сравнения с ТВ камерами на базе матриц ПЗС, где чувствительность приводится при отношении сигнал/шум 20 – 24 дБ, величины чувствительности в таблице 4 нужно уменьшить в 5 раз.

Таблица 6 – Основные параметры матриц ПЗС EMCCD фирм e2V и Texas Instruments, работающие при освещенности $\leq 10x10^{-6}$ лк

№ п/п	Фирма	Модель	Разрешение, число пикселей	Размер пикселя, мкм	Размер чувствительной области, мм	Тактовая частота, МГц	Корпус	Примечание
1	e2V	CCD60 (BI)	128x128	24	3,07x3,07	18	24-и контактный, DIL, керамический	
2	e2V	CCD97-00 (FI, BI)	512x512	16	8,19x8,19	15	30-и контактный, керамический	
3	e2V	CCD97-00 (BI)	512x512	16	8,19x8,19	15	С элементом Пельтье	
4	e2V	CCD201-20 (FI, BI)	10243x1024	13	13,3x13,3	20	36-и контактный, керамический	
5	e2V	CCD216-05 (BI)	768x244	11,5x27	8,83x6,59	15	С элементом Пельтье	
6	e2V	CCD216-08 (BI)	768x288	11,5x23	8,83x6,62	15	С элементом Пельтье	
Модели, поставляемые по специальному заказу, в т.ч. в исполнении для использования в космических условиях (SPASE QUALIFIED)								
7	e2V	CCD60 (BI)	128x128	24	3,07x3,07	18	С элементом Пельтье	
8	e2V	CCD65	576x288	20x30	11,5x8,6	16	36-и контактный PGA, керамический	
9	e2V	CCD201-20 (BI)	1024x1024	13	13,3x13,3	20	С элементом Пельтье	
10	e2V	CCD207-00 (FI, BI)	1632x208	15	16	15	Керамический	
11	e2V	CCD207-10 (FI, BI)	1632x408	15	16	15	Керамический	
12	e2V	CCD207-40 (BI)	1632x1608	15	16	15	38-и контактный, керамический	
13	Texas Instruments	Falcon BLUE TC285 SPD	1004x1002	8				Рабочая область спектра 0,18 – 1,1 мкм, частота кадров 30 Гц, время экспозиции до 500 мкс
14	Texas Instruments	Falcon TC285 SPD	1004x1002	8				Рабочая область спектра 0,35 – 1,1 мкм, частота кадров 30 Гц, время экспозиции до 500 мкс

Примечание: FI (Front Illumination) – фронтальная засветка, BI (Back Illumination) – обратная засветка, перенос – кадровый, рабочая область спектра 0,3 – 1,06 мкм, отношение сигнал/шум 35 дБ, диапазон рабочих температур для моделей 11 – 12 (-35) – (+55)°, для моделей 13 - 14 диапазон рабочих температур (-20) - (+55)°С, габариты 86x71x71 мм.

Таблица 7 – Основные параметры высокочувствительных ТВ камер на основе матриц ПЗС EMCCD

№ п/п	Фирма	Модель	Формат, дюймы	Число пикселей	Размер пикселя, мкм	Размеры активной поверхности, мм	Разрешение, ТВ линий	Рабочая область спектра, нм	Чувствительность, лк	Динамический диапазон, дБ	Масса, кг	Габариты, мм	Напряжение питания, В/энерго потребление, Вт	Диапазон рабочих температур, °С	Примечание
1	e2V	L3C216-05AFS		768x244	11,5x27			300 - 1060	10^{-5}	35		80x71x71		(-35) – (+55)	Есть ЖК затвор; ТВ стандарт 525 строк
2	e2V	L3C216-06AFS		768x288	11,5x23			300 - 1060	10^{-5}	35		80x71x71		(-35) – (+55)	Есть ЖК затвор; ТВ стандарт 625 строк
3	e2V	L3C216-05AFS1		768x244	11,5x27			300 - 1060	10^{-5}	35		80x71x71		(-35) – (+55)	Нет ЖК затвора; ТВ стандарт 525 строк
4	e2V	L3C216-06AFS1		768x288	11,5x23			300 - 1060	10^{-5}	35		80x71x71		(-35) – (+55)	Нет ЖК затвора; ТВ стандарт 625 строк
5	Raptor Photonics	MERLIN EM247	1/2	658x496	10x10	6,58x4,96		350 - 1100	10^{-5}	55	0,395	68x56x84	=12/12		Пиковая квантовая эффективность 52% на 530 нм, нелинейность менее 1 %, частота кадров 35 Гц, шум менее 1 электрона, темновой ток менее 0,1 электронов/пикселей/с, охлаждение до (-20)°С
6	Raptor Photonics	Hawk-EMCCD-210114	1/2	658x496	10x10	6,58x4,96	450	350 - 1100	$2x10^{-4}$	55	0,15	43x43x57	=12/<4,5 - 5	(-20) – (+(55)	Антиблюминговая защита более 500:1, частота кадров 35 Гц,
7	Raptor Photonics	Hawk EM 216-CB	2/3	769x288	11,5x28	8,832x6,624	625	180 - 1100	$5x10^{-5}$	55	0,23	50x45x75	=12/-	(-20) – (+(55)	
8	Raptor Photonics	Hawk CCDI	1/2	768x494	8,6x8,3	6,6x4,1	482	350 - 1100	$<10^{-6}$	>60	0,15	43x43x57	=12/-	(-20) – (+(55)	Частота кадров 25 Гц
9	Raptor Photonics	Hawk CCDII	1/2	752x582	8,6x8,3	6,47x4,83	482	350 - 1100	$<10^{-6}$	>60	0,15	43x43x57	=12/-	(-20) – (+(55)	Частота кадров 30 Гц
10	Raptor Photonics	Hawk 247-CL	1/2	658x496	10x10		450	350 - 1100	10^{-5}	55	0,15	43x43x57	=12/5	(-20) – (+(55)	Охлаждение – ТЭО, частота кадров 25/35 Гц
11	Raptor Photonics	Hawk 247-A	1/2	658x496	10x10		450	350 - 1100	10^{-5}	55	0,15	43x43x57	=12/4,5	(-20) – (+(55)	Охлаждение – ТЭО, частота кадров 25/35 Гц
12	Raptor Photonics	Hawk 216-A	2/3	769x288	11,5x27		625	180 - 100	10^{-5}	55	0,23	50x45x75	=12/8	(-20) – (+(55)	Охлаждение – ТЭО, частота кадров 25/35 Гц
13	Hamamatsu	ORCA-Flash 4.0		2048x2048	6,5x6,5			Видимая область спектра	10^{-5}						Квантовая эффективность более 70% на длине волны 600 нм и 50% на длине волны 750 нм, шум 1,3 электрона, частота кадров 100 Гц, время экспозиции 9,7 мкс – 10 с,
14	Hitachi	KP-DE500/KP-E500	1/2	680x500	10x10	6,58x4,96	480 (горизонт.) 380 (вертикальн.)		$9x10^{-3}$ (цветное изобр.) $5x10^{-3}$ (черно-белое изобр.) $1,5x10^{-4}$ (цветное изобр., 64-х суммирование) $8x10^{-6}$ (черно-белое суммирование)	50	0,53	78x63x170	=12/15	(-10) – (+50)	Относительное отверстие объектива 1:1,4, суммирование полей 2-х, 4-х, 6-х, 8-х, 10-х, 16-х, 32-х, 64-х, цифровая обработка изображения
15	Hitachi	KP-D500-S1 1/2"	1/2	658x489	10x10	6,58x4,89	480 (горизонт.) 350 (вертикальн.)		$9x10^{-3}$ (цветное изобр.) $5x10^{-3}$ (черно-белое изобр.) $1,5x10^{-4}$ (цветное изобр., 64-х суммирование) $8x10^{-6}$ (черно-белое суммирование)	50	0,61	78x63x170	=12/18	(-20) – (+60)	В модификации ТВ камеры DKP-M500 при относительном отверстии объектива 1:1,2 имеем минимальную рабочую освещенность $3x10^{-5}$ лк (без накопления) и $5x10^{-7}$ лк (с 64-х накоплением). Режим накопления выбирается ступенями от 2-х до 64-х (автоматически) или от 2-х до 128 (вручную). Электронный затвор имеет режимы экспозиции от 1/60 с до 1/2000 с.

Примечание: ТЭО – термоэлектическое охлаждение.

Литература

1. Волков В. Г. Сверхвысокочувствительные телевизионные системы // Специальная техника. 2002. № 4. С. 2-11.

2. Волков В. Г. Телевизионные камеры для спецтехники // Спецтехника и связь. 2009. № 1. С. 2-11.

3. Волков В. Г. Цифровые приборы ночного видения // Спецтехника и связь. 2013. № 3. С. 13.

4. Гейхман И. Л., Волков В. Г. Видение и безопасность. – М.: Новости. 2009. – 840 с.

5. Волков В. Г., Гиндин П. Д. Техническое зрение. Инновации. – М.: Техносфера, 2014. – 840 с.

6. Телекамеры SMARTEC премиум-класса серии ULTIMATE // Smartec CCTV [Электронный ресурс]. 2016. – URL: www.smartec-cctv.ru (дата обращения 01.07.2016).

7. Телевизионные камеры фирмы ЭВС // Сайт компании ЭВС [Электронный ресурс]. 2016. – URL: www.evs.ru (дата обращения 22.07.2016).

8. Телевизионные камеры. Системы видеонаблюдения. Каталог фирмы ЭВС. – СПб.: ЭВС, 2016.

9. Высокочувствительные и мегапиксельные телекамеры НПФ «ЭВС» // S-Прогресс [Электронный ресурс]. 2016. – URL: http://sio.su/down_006_111_def.aspx (дата обращения 01.07.2016).

10. ТВ камеры с повышенной чувствительностью. Каталог ОАО «НПО Геофизика-НВ». – М.: НПО Геофизика-НВ», 2016.

11. ТВ камера «Кречет». Проспект фирмы ОАО «ЦНИИ ЦИКЛОН». – М.: ОАО «ЦНИИ ЦИКЛОН», 2014.

12. Матрицы ПЗС EMCCD и ТВ камера MERLIN на их основе // E2V [Электронный ресурс]. 2016. – URL: http://www.diaworld.ru/catalog/merlin_em247.pdf (дата обращения 02.07.2016).

13. Научные CCD видеокамеры Falcon фирмы Raptor Photonics // Raptor Photonics [Электронный ресурс]. 2016. – URL: www.raptorphotonics.ru (дата обращения 03.07.2016).

14. Казначеев С. А. особенности получения ТВ-изображений при ограниченных потоках фотонов // Наука и образование. 2014. № 6. С. 209-221. – URL: http://technomag.bmstu.ru/djc/716587.html (дата обращения 03.07.2016).

15. CCD97-00. Back Illuminated 2-Phase IMO Series Electron Multiplying CCD Sensor // E2V [Электронный ресурс]. 2011. – URL: http://www.e2v.com/resources/account/download-datusheet/1487 (дата обращения 04.07.2016).

16. ТВ камера на основе EMCCD черно-белого изображения MERLIN EM247 // Фирма Raptor Photonics [Электронный ресурс]. 2016. – URL: www.diawirld.ru (дата обращения 04.07.2016).

17. ТВ камера ORCA-Flash 4.0 меняет правила игры // Проспект фирмы Hamamatsu. 2016.

18. Максимов А. Ф., Балега Ю. Ю., Дьяченко В. В., Малоголовец Е. Р., Расстегаев В. А., Семерников Е. М. Спекл-интерферометр 6-м телескопа САО РАН на основе EM CCD: характеристики и новые результаты // Астрофизический бюллетень. 2009. Т. 64. № 3. С. 308-221.

19. Комаров В. В. EM CCD CCTV камеры – исследование по небесным объектам // Прикладная физика. 2012. № 2. С. 99-103.

References

1. Volkov V. G. Sverchvisokochuvstvitelnye televisionnye systemy [Superhighsensitivity television system]. *Spetsial'naia Tekhnika*, 2002, no. 4, pp. 2-11 (in Russian).

2. Volkov V. G. Televisionnye camery dlja speztechniky [Television cameras for construction equipment]. *Specialized Machinery and Communication*, 2009, no. 1, pp. 2-11 (in Russian).

3. Volkov V. G. Zifrovye pribory nochnogo videnija [Digital night vision devices]. *Specialized Machinery and Communication*, 2013, no. 3, pp. 13 (in Russian).

4. Gaykhman I. L., Volkov V. G. *Videnie i besopasnost* [Vision and safety]. Moscow, News Publ., 2009. 840 p. (in Russian).

5. Volcov V. G., Gindin P. D. *Technicheskoe zrenye. Innjvazyi* [Technical vision. Innovation]. Moscow, Tekhnosfera Publ., 2014. 840 p. (in Russian).

6. Telecamery SMARTEC premium classa seryi ULTIMATE [The camera SMARTEC premium series ULTIMATE]. *Smartec CCTV*, 2016. Available at: www.smartec-cctv.ru (accessed 01 June 2016) (in Russian).

7. Televisionnye camery Kompanyi EVS. [Television Cameras company the EVS]. *EVS Sait*, 2016. Available at: www.evs.ru (accessed 22 June 2016) (in Russian).

8. *Televisionnye camery. Systemy videonabludenyja* [TV Cameras. A video surveillance systems]. Saint-Petersburg, EVS Company Publ., 2016.

9. Vysokochuvstvitelnye i megapixelnye camery firmy “EVS” [Highly sensitive and megapixel cameras NPF "EVS"]. S-Progress, 2016. Available at: http://sio.su/down_006_111_def.aspx (accessed 01 June 2016) (in Russian).

10. Televisionnye camery s povishennoy chuvstvitelnostju [TV cameras with high sensitivity]. Moscow, Catalogue of JSC "NPO Geofizika-NV", 2016. (in Russian).

11. Televisionnaya camera “Krechet” [TV camera "Merlin"]. Moscow, Prospect of the “TSNII CYCLONE" company, 2014. (in Russian).

12. Matrizy EMCCD CCD b televisionnaja camera MERLIN na ich osnove. [The EMCCD CCD matrix and TV camera MERLIN based on them]. E2V, 2016. Available at: http://www.diaworld.ru/catalog/merlin_em247.pdf (accessed 02 June 2016) (in Russian).

13. Nauchnye CCD camery Falcon kompanyi Raptor Photonics [Scientific CCD cameras Falcon company Raptor Photonics]. Raptor Photonics, 2016. Available at: www.raptorphotonics.ru (accessed 03 June 2016). (in Russian).

14. Kaznacheev S. A. Osobennosty poluchenyja TV-izobrajoenyyj pri ogranichennom potoke photonov. [Peculiarities of obtaining TV images with a limited photon flux]. *Science and education*, 2014, vol. 6, pp. 209-221. Available at: http://technomag.bmstu.ru/djc/716587.html (accessed 03 July 2016) (in Russian).

15. CCD97-00. Back Illuminated 2-Phase IMO Series Electron Multiplying CCD Sensor. *E2V Technologies Ltd.*, 2011. Available at: http://www.e2v.com/resources/account/download-datusheet/1487 (accessed 04 July 2016). (in Russian).

16. TV camera na osnove EM CCD cherno-belogo izobrajoenyja MERLIN EM 247 [TV camera on the basis of the EMCCD monochrome image MERLIN EM247]. *Firm Raptor Photonics*, 2016. Available at: www.diawirld.ru (accessed 04 July 2016) (in Russian).

17. TV camerra ORCA-Flash4.0 menjaet pravila igry [TV camera ORCA-Flash4.0 game-changing]. *The prospect of the Hamamatsu company*, 2016. (in Russian).

18. Maksimov A. F., Balega V. V., Dyachenko E. R., Malogolovets V. A., Rasstegaev V. A., Semernikov E. M. Speckl-interferometer 6 m telescope SO RAN na osnove EM CCD: chracteristiky I novye resultaty [The speckle interferometer of the 6-m telescope of Sao RAS on the basis of the EM CCD: characteristics and new results]. *Astrophysical Bulletin*, 2009, vol. 64, no. 3, pp. 308-221 (in Russian).

19. Komarov V. V. EM CCD TV camery – issledovanija po nebesnym objektam [EM CCD cameras CCTV – the study of celestial objects]. *Prikladnaia fizika*, 2012, no. 2, pp. 99-103 (in Russian).

Статья поступила 18 июля 2016 г.

Сведения об авторе

Волков Виктор Генрихович – доктор технических наук, академик Российской Академии Естественных Наук, профессор кафедры РЛ-2 «Лазерные и оптико-электронные системы». Московский Государственный Технический Университет имени Н.Э. Баумана. Область научных интересов: приборы визуализации изображения. E-mail: volkvik2009@yandex.ru

Адрес: Россия, 105005, г. Москва, ул. 2-я Бауманская, д. 5, стр. 1.

High-Sensitivity Television Camera for Security

V. G. Volkov

Problem statement. *The new highly sensitive television (TV) cameras which ensure the work of the security services, are describes in the paper. Also, their technical parameters and potentialities are described in paper.* ***Objective.*** *The analysis of a latest developments in the field of creation of specific TV cameras of various types for ensure safety is aim of paper. Methods of analysis are the scientific comparison and the technical analysis of the capabilities of the TV cameras and methods their application in security systems.* ***Novelty.*** *The systematic analysis of the technical parameters for the high-sensitivity TV cameras which uses as safety devices is novelty of paper.* ***Practical significance.*** *Methods of use of the high sensitivity TV cameras are offer for the security systems. The methods are selected according of the parameters cameras, their ability to provide around the clock monitoring and operation in degraded conditions vision.*

Keywords: *TV, camera, sensitivity, signal/noise, resolution, dynamic range, pixel size, size of the active area, mass, size, energy consumption.*

About the Author

Viktor Genrichovich Volkov – Dr. habil. of Engineering Sciences, Academician of Russian Academy of Natural Sciences. Professor at the Department RL-2 “Laser and Optic Electron Systems”. Bauman Moscow State Technical University. Field of research: devices of images visualization. E-mail: volkvik2009@yandex.ru

Address: Russia, 105005, Moscow, 2nd Baumanskaya str., 5-1.

УДК 623.624

Информационные конфликты – анализ работ и методологии исследования

Макаренко С. И., Михайлов Р. Л.

Актуальность. *В настоящее время ведется формирование методологии теории информационного противоборства в технической сфере как закономерного развития теорий радиоэлектронной борьбы и информационной безопасности. При этом создание и развитие научно-методического аппарата информационного противоборства тесно связано с теорией конфликтов, в частности с методологией исследований информационного конфликта. В связи с этим, актуальным является анализ известных работ и методологии исследования информационного конфликта.* ***Целью работы*** *является анализ известных публикаций в области методологии исследования информационного конфликта. Особое внимание уделено анализу конфликта наблюдения и конфликта подавления, применительно к системам связи.* ***Используемые методы.*** *Решение задачи основано на использовании методов индукции и дедукции теории логики.* ***Результат.*** *На основе анализа более 300 источников выявлены общие и частные закономерности исследования информационного конфликта на основе использования различного научно-методического аппарата, а именно: теории активных систем, теории динамических систем, теории игр, теории марковских процессов, теории сетей Петри, теории сложных иерархических систем, а также других теорий. Показано, что актуальными направлениями развития исследований информационного конфликта являются: учет факторов сложности и многоуровневости конфликтующих систем, многоэтапности протекания конфликта; учет скрытых воздействий в процессе конфликта, а также учет динамических свойств конфликта, за счет его формализации на основе теории динамических систем, теории бифуркации, теории катастроф и теории детерминированного хаоса.* ***Новизна.*** *Элементами новизны работы являются выявленные общие и частные закономерности и подходы к исследованию информационного конфликта на основе использования различного научно-методического аппарата. Также к элементам новизны стоит отнести выявленные частные тенденции исследования информационных конфликтов в областях радиомониторинга и радиоэлектронного подавления в приложении к системам связи.* ***Практическая значимость.*** *Представленный анализ может быть использован техническими специалистами для обоснования новых технологических решений в области радиоэлектронной борьбы, информационного противоборства, радиомониторинга и систем связи, а также военными специалистами – для обоснования новых форм и способов вооруженной борьбы с учетом перспектив развития информационного конфликта. Кроме того, данный анализ будет полезен научным работникам и соискателям, ведущим научные исследования в области информационного конфликта.*

Ключевые слова: *конфликт, информационный конфликт, система связи, радиоэлектронная борьба, радиомониторинг, информационное противоборство.*

Актуальность

В настоящее время ведется формирование методологии теории информационного противоборства в технической сфере как закономерного развития ранее разобщенных теорий радиоэлектронной борьбы и информационной безопасности. При этом создание и развитие научно-методического аппарата информационного противоборства тесно связано с теорией конфликтов, в частности с методологией исследований информационного конфликта.

Исследования конфликтов в различных прикладных областях

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].

Изучению конфликтов систем в различных прикладных областях посвящены работы: В.М. Гаврилова [2], В.Ф. Крапивина [3], В.А. Лефевр [4], Т.Л. Саати [5], М. Месаровича, И. Такахара [6, 7], Н.Н. Данилова [8], Е.Л. Берзина [9], Н.С. Кукушкина [10], В.А. Горелика, М.А. Горелова, А.Ф. Кононенко [12], А.А. Чикрий [13], В.Н. Буркова [14, 15], В.А. Ирикова [15], О.А. Малафеева, А.И. Муравьева [16], В.А. Светлова [17], В.И. Новосельцева [18], Д.А. Новикова [19-22], А.Г. Чхартишвили [20], Д.А. Губанова [22], Л.Е. Мистрова [24, 26, 47, 48, 239, 240], Ю.С. Сербулова [23, 25, 26], Г.А. Угольницкого [27, 28, 29], А.Б. Усова [28-30], У. Детмера [31], Г.И. Алгазина [32, 33, 34], В.И. Жуковского [35, 36], В.В. Сысоева, Д.В. Сысоева [37-41], В.В. Дружинина, А.С. Конторова, Д.С. Конторова [57, 58], Н.Н. Воробьева [367], D.A. Blackwell, M.A. Girshick [372], J.M. Danskin [373], J. Neumann, O. Morgenstern [374], Т. Партхасаратхи, Т. Рагхаван [375], Л.А. Петросяна [180, 376], Г.В. Томского [376], Ф.Л. Черноусько, А.А. Меликяна [377], а также других ученых.

К интересным исследованиям, которые развивают классические труды в области теории конфликтов, можно отнести следующие работы.

Работы Д.В. Сысоева и В.В. Сысоева [37-41], которые посвящены структурно-параметрическому взаимодействию подсистем, в результате которого формируется класс так называемых приведенных систем. Кроме того, в них рассмотрены свойства независимости подсистем в целом, алгоритмы построения приведенных систем, а также формализованы области конфликтного взаимодействия и особенности выбора решений в них.

В работе М.И. Рубинштейна [42] с единых позиций рассматриваются детерминированные задачи распределения группировки противостоящих сторон. Описываются общая модель и практически важные частные модели детерминированных задач группировки конфликтующих сторон, приводятся их содержательные интерпретации. Для решения этих задач рассматривается применение общих методов дискретного программирования.

В работах М.Е. Корягина [43, 44] предложена модель оптимизации управления конфликтной системой на основе поиска конфликтного равновесия

между сторонами с различными интересами, а также ее приложение для управления городским пассажирским транспортом. Показано, что в случае, если целью конфликта является овладение одной из сторон каким-либо ресурсом (или распределения ограниченного ресурса в случае неантагонистического конфликта между всеми сторонами), то такую задачу можно свести к задаче оптимального распределения ресурсов.

Вопросы распределения ресурсов на основе конфликтного взаимодействия различных организационно-технических систем рассмотрены в работах Е.Л. Берзина [9], Л.С. Гурина, Я.С. Дымарского, А.Д. Меркулова [45], Б.А. Гусейнова, И.А. Ушакова [46], Л.Е. Мистрова [47, 48].

В работе С.В. Величко, Ю.С. Сербулова, А.В. Лемешкина [26] обобщены полученные другими исследователями результаты и предложены изящные модели и методы распределения ресурсов с использованием как системного, так и теоретико-игрового подходов. Отмечается, что решение ресурсных задач связано с двумя основными аспектами: проблемой выбора и проблемой распределения ресурсов, в рамках которых происходит назначение каждому элементу организационно-технической системы определенных видов и объемов конкретных ресурсов. Необходимость решения этих проблем связана с тем, что любой системе для достижения поставленных перед ней целей требуются различные ресурсы, количество которых ограничено. При этом могут возникать конфликты ресурсного взаимодействия как между организационно-техническими системами, так и между их подсистемами, в том числе и ресурсный конфликт. Последний случай при условии ограниченности ресурсов наиболее типичен для реальной организационно-технической системы. Таким образом, ресурсная конкуренция выступает фактором ее функционирования и динамики развития. Несоответствие между целями системы и ее ресурсами, которые необходимы для их достижения, определяет проблему выбора и распределения ресурсов, а именно – синтез ресурсного компромисса в организационно-технической системе.

При приложении теории конфликта к моделированию современных организационно-технических систем необходимо также учитывать такие их свойства, как сложность и моногоуровневость. К исследованиям, в которых рассматриваются конфликты с учетом фактора сложного иерархического построения организационно-технических систем, можно отнести работы: М. Месаровича, Д. Мако, И. Такахары [6], Д.А. Новикова [21], Л.Е. Мистрова, Ю.С. Сербулова [23], Г.А. Угольницкого [27-29], Г.И. Алгазина [34], В.В. Дружинина, А.С. Конторова, Д.С. Конторова [57, 58], В.И. Владимирова [60], Ю.Л. Козирацкого [1, 61], В.Г. Радзиевского [74], Нгуена Куанга Тхыонга [189], С.И. Макаренко [54].

Анализ и классификация общетеоретических работ в области конфликтов представлен на рис. 1.

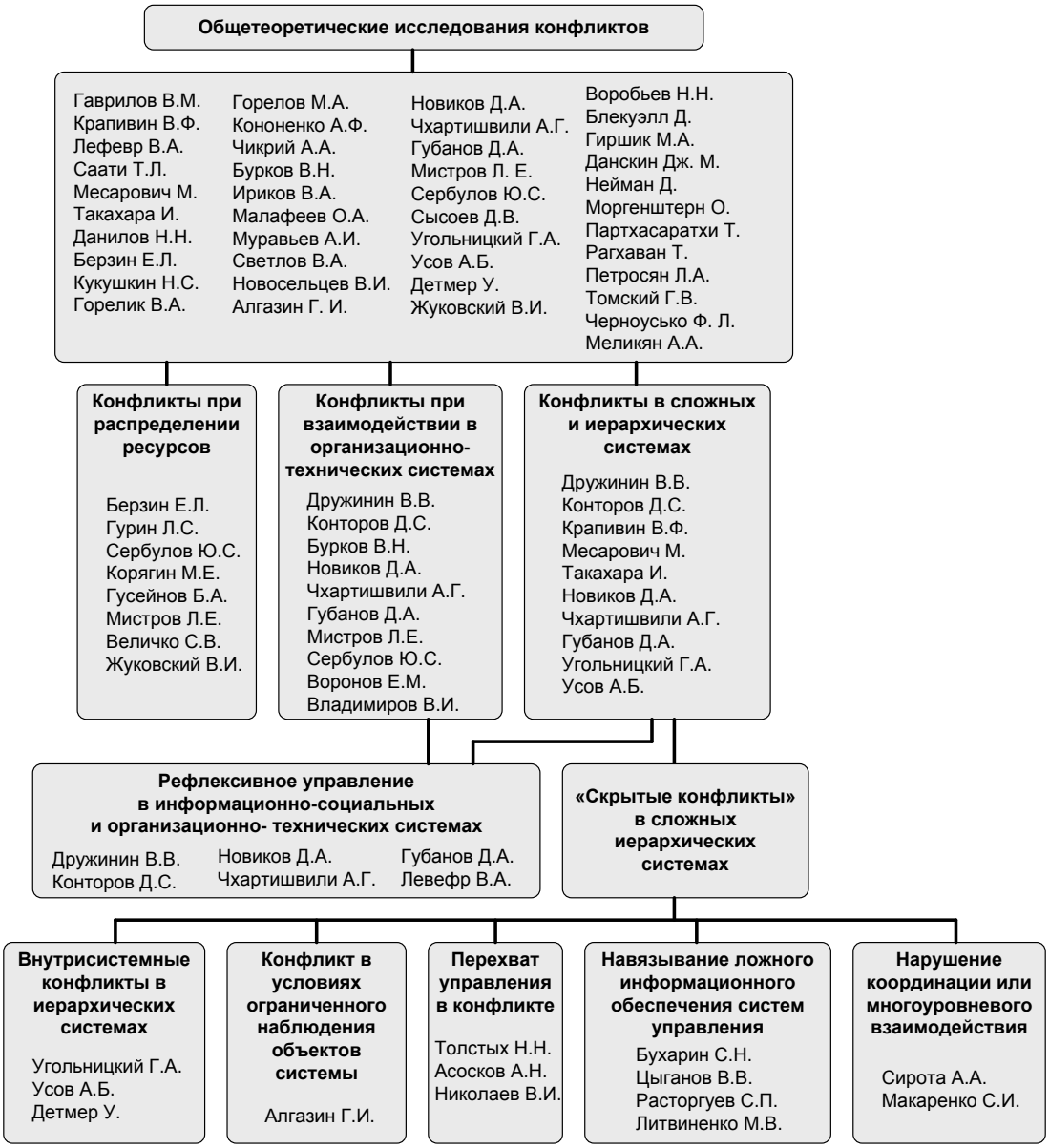


Рис. 1. Общетеоретические работы в области конфликтов

Отдельно нужно отметить исследования так называемого «скрытого конфликта» в случаях, когда конфликтующими сторонами являются сложные системы, и каждая из них осуществляет скрытые воздействия, направленные на формирование и развитие внутрисистемных локальных мини-конфликтов в структуре и функционировании системы противостоящей стороны. Такие скрытые воздействия могут быть связанны с различными аспектами функционирования сложных систем:

- формированием различных целей у объектов (подсистем и элементов конфликтующих систем) и ограничение их доступа к внутренним ресурсам (работа У. Деттмер [31]);
- ограничением наблюдаемости объектов (работы Г.И. Алгазина [32-34]);

- формированием ложных целей у объектов с целью развития межуровневых конфликтов внутри системы (работы А.Б. Усова и Г.А. Угольницкого [27-30]);
- навязыванием ложного информационного обеспечения систем управления (данный вид воздействия широко рассматривается в исследованиях по информационному противоборству в работах: С.Н. Бухарина, В.В. Цыганова [49], С.П. Расторгуева, М.В. Литвиненко [50]);
- перехватом управления отдельными объектами или системой в целом (работы Н.Н. Толстых [51, 347], А.Н. Асоскова [52], В.И. Николаева [347]);
- нарушением координации или многоуровневого взаимодействия между объектами в системе (работы А.А. Сироты [250], С.И. Макаренко [54]).

Исследования информационного конфликта

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 Д.А. Новикова [55]. В работе В.О. Ашкеназы [56] представлен обзор работ зарубежных (в основном американских) авторов, которые охватывают моделирование широкого диапазона военных конфликтов на основе теории игр (в том числе дифференциальных игр) и теории исследования операций. Отдельным аспектам моделирования военных конфликтов посвящены работы Т.Л. Саати [5], В.В. Дружинина, А.С. Конторова, Д.С. Конторова [57, 58], Е.М. Воронова [59], J.M. Danskin [373].

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 систем управления силами и оружием.

Информационный конфликт – 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 [1].

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* [60, 61]. Дуэль долгое время являлась основным элементом конфликта в РЭБ. При этом, в связи с переходом к сетецентрическому управлению военными действиями, в настоящее время наблюдается переход от моделей на основе дуэлей к моделям на основе столкновений нескольких сторон, находящихся в различной степени конфликтности (таких как: антагонистический конфликт, враждебность, нейтралитет, союзничество, симбиоз).

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

Первоначальные исследования в области информационного конфликта описывали взаимодействие средств подавления и *радиолокационных систем*. К таким исследованиям относятся работы: С.А. Вакина [62], Л.Н. Шустова [62, 69], М.В. Максимова [63], В.В. Дружинина, Д.С. Конторова [64], А.И. Палия [65], В.В. Цветнова, В.П. Демина [66, 67], А.И. Куприянова [66, 67, 68, 69, 70], А.В. Сахарова [68], Ю.М. Перунова, [71, 72] К.И. Фомичева, Л.М. Юдина [71], В.В. Мацукевича, А.А. Васильева [72], В.Г. Радзиевского [73, 74], В.М. Шляхина [75-79], Ю.С. Сухорукова [75, 76], В.И. Владимирова [60, 77], В.П. Лихачева [77], А.И. Канащенкова, В.И. Меркулова [80, 349-351], Ю.П. Мельникова [81], Б.А. Никольского [53], А.В. Леньшина [99], С.В. Ягольникова [343-345], А.А. Вакуленко [333, 343, 344, 346], В.С. Вербы [343, 346, 348], В.И. Шевчука [333, 345] и других ученых.

Расширение предметной области ведения РЭБ привело к разработке методологии информационного конфликта применительно к другим системам, а именно:

- *системам навигационного обеспечения* – работы: В.Г. Радзиевского [82, 83], В.А. Миронова [82-84], Ю.М. Перунова, В.В. Мацукевича, А.А. Васильева [72], А.П. Дятлова, Б.Х. Кульбикаяна [85, 86], П.А. Дятлова [86];
- *системам радио и радиотехнического мониторинга* – работы: Ю.Л. Козирацкого [1, 98], С.А. Вакина [62], Л.Н. Шустова [62, 69], В.А. Вартанесяна [87], Ю.М. Перунова, В.В. Мацукевича, А.А. Васильева [72], В.В. Цветнова, [66, 67], В.О. Демина [66, 67, 88], А.И. Куприянова [66, 67, 88], А.В. Сахарова [68, 88], В.Г. Радзиевского [74, 89-92], А.А. Сироты [89-95], Ю.А. Борисова [93, 95], В.И. Владимирова [60, 77], В. П. Лихачева, В.М. Шляхина [77], С.В. Дворникова [97, 198, 199], А.П. Дятлова, П.А. Дятлова, Б.Х. Кульбикаяна [85, 86, 100], А.И. Рембовского, А.В. Ашихмина, В.А. Козьмина [101], Ю.К. Меньшакова [102, 103], Ю.П. Мельникова [81], Ю.С. Лифанова, В.Н. Саблина, М.И. Салтана [104], А.А. Вакуленко, В.С. Вербы [105], В.Л. Гребенюка, В.В. Исаева, В.Ф. Мельникова [106], А.Н. Борисова [191-193], А.А. Алексеева [192, 195], Ю.А. Смирнова [194], Б.А. Никольского [53], В.Д. Челышева, В.В. Якимовца [196], Л.А. Марчука [197], А.Н. Захарченко [200], В. И. Кононова [201], А.И. Замарина, Д.А. Тавалинского [202, 203], Р.В. Волкова [204];
- *системам технической и компьютерной разведки* – работы: Ю.К. Меньшакова [102, 103], А.А. Хореева [107], А.И. Куприянова, А.В. Сахарова, В.А. Шевцова [108], В.И. Аверченкова, М.Ю. Рытова, А.В. Кувыклина, Т.Р. Гайнулина [109], И.И. Чукляева, А.В. Морозова [110], Б.С. Гольдштейна [111], П.Н. Девянина [112], А.С. Пахомовой [113, 114], Е.В. Гречишникова [276], А.А. Привалова [352, 354, 357], Н.В. Евглевской [352, 354], Е.В. Скудневой [357];
- *системам оптического наблюдения* – работы: Ю.Л. Козирацкого [1], В.Г. Радзиевского [74], Ю.К. Меньшакова [102, 103];
- *системам радиосвязи* – работы: А.Г. Зюко [116], В.И. Коржика, М.М. Финка, К.Н. Щелкунова [117], А.И. Палия [65], Г.И. Тузова [118], М.В. Максимова [63], Ю.М. Перунова, В.В. Мацукевича, А.А. Васильева [72], В.И. Владимирова [60, 77, 121-125], В.И. Борисова, В.М. Зинчука [119, 120], А.Е. Лимарева, А.В. Немчилова, А.А. Чаплыгина [120], В.Г. Радзиевского [74], А.И. Куприянова [68, 69], Л.Н. Шустова [69], А.В. Сахарова [68], А.А. Привалова [115], М.А. Семисошенко [126], А.М. Чуднова [127-129, 368], П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко [129], Д.Л. Бураченко [130], В.И. Кузнецова [132], А.В. Боговика, В.В. Игнатова [133], Е.Е. Исакова [134], С.М. Одоевского, В.И. Калюки [135], В.И. Николаева, А.Е. Фёдорова [136, 137], Е.А. Шабалина [138, 139], Н.М. Радько, А.Н. Мокроусова [140], Г.Н. Мальцева, В.В. Вознюка, М.Р. Туктамышева [141],

М.И.Жодзишского [369], Д.Г. Козлова [378], А.Н. Путилина [379-381] и других ученых.

Обобщенная схема исследований в области информационного конфликта представлена на рис. 2.

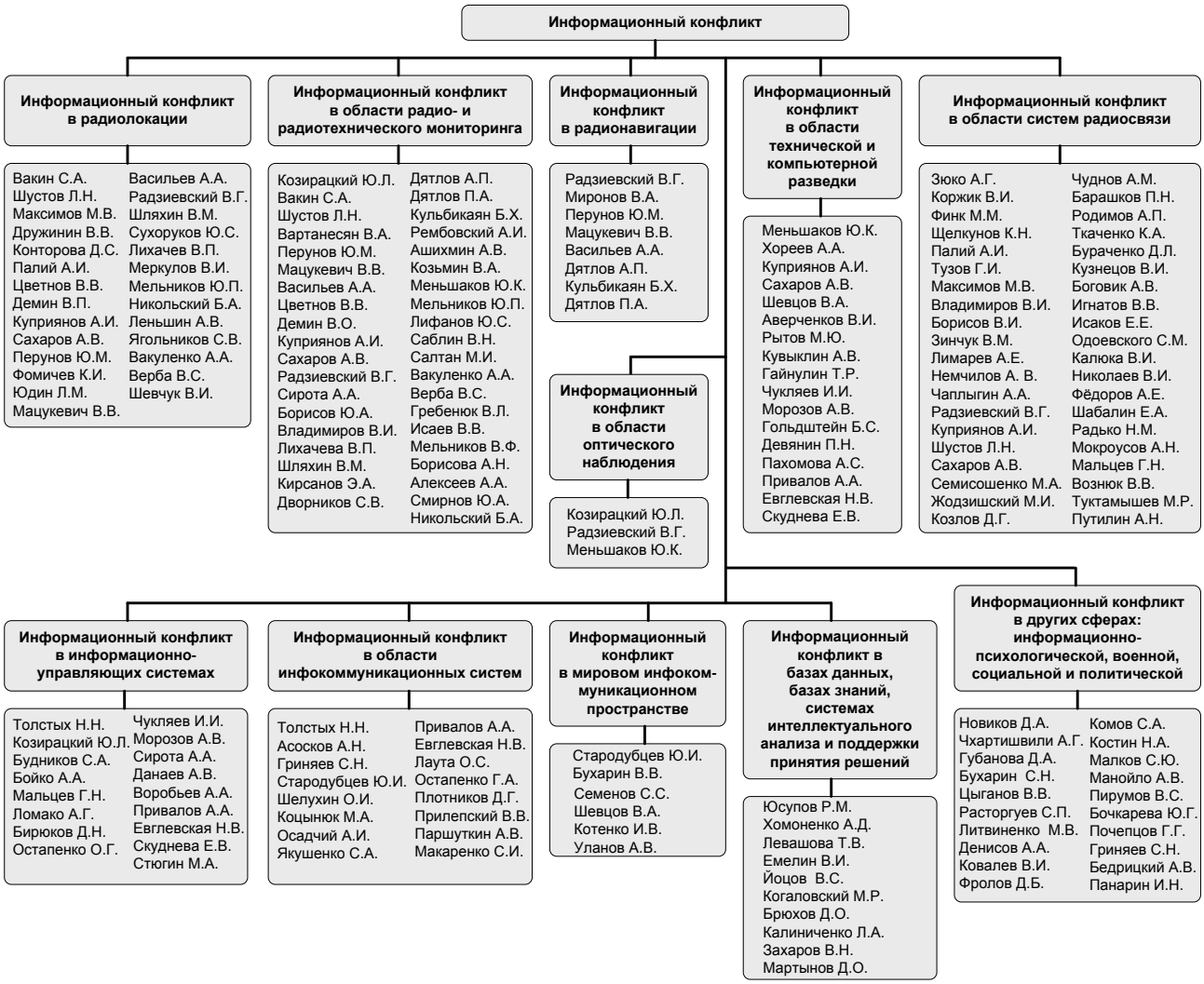


Рис. 2. Обобщенная схема исследований информационного конфликта в различных предметных областях

Помимо тематики РЭБ областью соответствующей информационному конфликту является методология информационного противоборства в технической сфере. Эта область в настоящее время активно развивается, при этом само противоборство можно отнести к отдельному типу проявления информационного конфликта в новых прикладных областях, а именно:

- *информационно-управляющих систем* – работы: Н.Н. Толстых [142], Ю.Л. Козирацкого [98, 241, 242], С.А. Будникова [143, 144, 246], А.А. Бойко [145, 146, 246, 247], Г.Н. Мальцева [147, 148], А.Г. Ломако, Д.Н. Бирюкова [149-153], О.Г. Остапенко [168-170], И.И. Чукляева, А.В. Морозова [154-156], А.А. Сироты [249, 250], А.В. Данаева, А.А. Воробьева [260], А.А. Привалова, Н.В. Евглевской, Е.В. Скудневой [353, 355] и других ученых;

- *мирового инфокоммуникационного пространства* – работы: Ю.И. Стародубцева, В.В. Бухарина, С.С. Семенова [157-160], В.А. Шевцова [257], И.В. Котенко, А.В. Уланова [340-342] и других ученых;
- *инфокоммуникационных систем* – работы: Н.Н. Толстых [51, 251, 252, 268], А.Н. Асоскова [52], С.Н. Гриняева [161], Ю.И. Стародубцева [162-164], О.И. Шелухина [165], М.А. Коцынюка, А.И. Осадчего, О.С. Лауты [166, 167], Г.А. Остапенко [170], В.В. Прилепского [235], С.А. Якушенко [259], А.В. Паршуткина [262, 263], А.А. Привалова, Н.В. Евглевской [354, 356], С.И. Макаренко [54] и других ученых;
- *в базах данных, знаний, а также в системах интеллектуального анализа и поддержки принятия решений* – работы: В.С. Йоцова [171, 359], Р.М. Юсупова, А.Д. Хомоненко [171], Т.В. Левашовой [96], В.И. Емелина [172], М.Р. Когаловского [360], Д.О. Брюхова, Л.А. Калиниченко, В.Н. Захаров, Д.О. Мартынова [361], А.М. Андреева, Д.В. Березкина, Ю.А. Кантонистов [362] и других ученых.

Кроме того, ведутся исследования по развитию методологии информационного конфликта в психологической и социально-политических сферах (работы Д.А. Новикова, А.Г. Чхартишвили, Д.А. Губанова [22], С.Н. Бухарина, В.В. Цыганова [173], С.П. Расторгуева, М.В. Литвиненко [50, 174]).

Вышеприведенные и другие известные работы в области конфликта (прежде всего информационного) основываются на научно-методическом аппарате:

- *теории активных систем* – работы: В.Н. Буркова [14, 15], Д.А. Новикова [21], С.П. Расторгуев [174], В.В. Поповского, А.В. Лемешко, О.Ю. Евсеевой [176] и других ученых;
- *теории динамических систем* – работы: В.М. Гаврилова [2], Н.Н. Толстых [51, 251, 252, 268], А.Н. Асоскова [52], Г.А. Остапенко, Д.Г. Плотникова, Ю.Н. Гузева [363-366] и других ученых;
- *теории игр* – работы: Д.А. Новикова [19], А.М. Чуднова [127-129, 368], С.М. Одоевского, В.И. Калюки [135], М.А. Семисошенко [126], И.И. Чукляева [154], В.И. Николаева, А.Е. Фёдорова [136, 137], С.А. Якушенко [259], А.В. Данеева, А.А. Воробьёва, Д.М. Лебедева [260], М.И. Жодзишского [369], T. Bazar [370], C. Cahn [371], Д.Г. Козлова [378], А.Н. Путилина [379-381] и других ученых;
- *теории дифференциальных игр* – работы: Р. Айзекса [177], Л.С. Понтрягина [178], Н.Н. Красовского, А.И. Субботина [179], Л.А. Петросяна [180], В.И. Жуковского [35, 36], Э.Р. Смольякова [183], Н.Н. Петрова, А.И. Благодатских [184] и других ученых;
- *теории марковских процессов*, в том числе полумарковских и вложенных марковских процессов – работы: В.И. Владимирова [60, 77, 121, 125], В.И. Борисова, В.М. Зинчука [119, 120], В.Г. Радзиевского

[74, 89, 90], А.А. Сироты [89, 90], Ю.Л. Козирацкого, С.А. Будникова [1], А.А. Бойко [146], А.А. Привалова [355] и других ученых;

- *теории сетей Петри* – работы: С.М. Климова, М.П. Сычёва, А.В. Астрахова [217], Н.М. Радько [140], Г.Н. Мальцева, М.Р. Тухтамышева [141], Ю.К. Язова, А.Л. Сердечного, А.В. Бабурина [222], С.А. Юдицкого [185], С.А. Будникова [245] и других ученых;
- *вероятностные сети* – работы: А.А. Привалова [115], М.А. Коцыняка, О.С. Лауты [166, 167] и других ученых;
- *теории автоматов* – работы: П.Н. Девянина [112], С.А. Юдицкого [186], В.И. Левина [237, 238] и других ученых;
- *теории сложных иерархических систем* – работы: М. Месаровича, И. Такахары [6, 7], Д.А. Новикова [187, 188], Л.Е. Мистрова, Ю.С. Сербулова [23], Г.А. Угольницкого [27-29], Г.И. Алгазина [34], Нгуена Куанга Тхыонга [189], Ю.Л. Козирацкого, С.А. Будникова [1, 61], В.И. Владимирова [60], В.Г. Радзиевского [74]), С.И. Макаренко [54] и других ученых;
- *теории логики* – работы: В.И. Левина [236, 358], Е.А. Немковой [358], Т.А. Тарана [190] и других ученых;
- *теории многоагентного моделирования* – работы: И.В. Котенко, А.В. Уланова [340-342] и других ученых;
- *теории нечетких множеств* – работы А.Н. Борисова [191-193], М.И. Тенетко и других ученых;
- *теории графидинамических многоагентных триадных сетей* – работы С.А. Юдицкого [185, 186, 382].

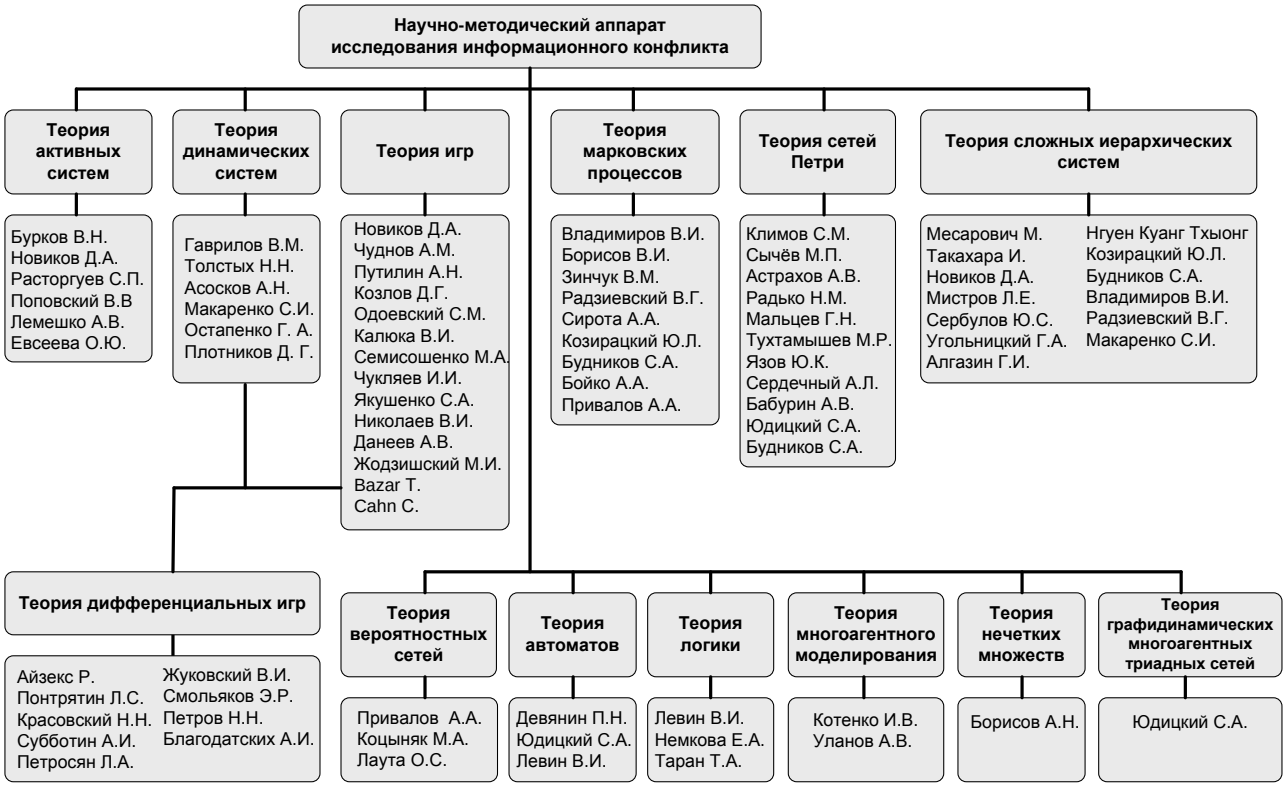


Рис. 3. Классификация исследований информационного конфликта по используемому научно-методическому аппарату

Обобщенная схема исследований учеными, ведущими исследования в области информационного конфликта, и их классификация по используемому ими научно-методическому аппарату представлена на рис. 3.

Рассмотрим далее отличительные особенности методологии исследования информационного конфликта наблюдения (применительно к средствам радиомониторинга) и информационного конфликта подавления (применительно к средствам связи).

Информационный конфликт систем связи в прикладной области радиомониторинга

Вопросам радиомониторинга посвящены работы: Ю.Л. Козирацкого [1, 98], С.А. Вакина [62], Л.Н. Шустова [62, 69], В.А. Вартанесяна [87], Ю.М. Перунова, В.В. Мацукевича, А.А. Васильева [72], В.В. Цветнова, [66, 67], В.О. Демина [66, 67, 88], А.И. Куприянова [66, 67, 88], А.В. Сахарова [68, 88], В.Г. Радзиевского [74, 89-92], А.А. Сироты [89, 90-95], Ю.А. Борисова [93, 95], В.И. Владимирова [60, 77], В.П. Лихачева, В.М. Шляхина [77], С.В. Дворникова [97, 198, 199], А.П. Дятлова, П.А. Дятлова, Б.Х. Кульбикаяна [85, 86, 100], А.И. Рембовского, А.В. Ашихмина, В.А. Козьмина [101], Ю.К. Меньшакова [102, 103], Ю.П. Мельникова [81], Ю.С. Лифанова, В.Н. Саблина, М.И. Салтана [104], А.А. Вакуленко, В.С. Вербы [105], В.Л. Гребенюка, В.В. Исаева, В.Ф. Мельникова [106], А.Н. Борисова [191-193], А.А. Алексеева [192, 195], Ю.А. Смирнова [194], Б.А. Никольского [53], В.Д. Челышева, В.В. Якимовца [196], Л.А. Марчука [197], А.Н. Захарченко [200], В.И. Кононова [201], А.И. Замарина, Д.А. Тавалинского [202, 203], Р.В. Волкова [204].

В вышеуказанных работах подробно рассматриваются вопросы повышения информационной доступности систем связи противоборствующей стороны, при этом всю совокупность работ можно декомпозировать на два основных направления исследований:

1) совершенствование технических аспектов добывания;
2) разработка оперативно-тактических требований к группировке сил и средств радиомониторинга при ведении специальной работы.

В работах В.А. Вартанесяна [87], А.И. Куприянова [66, 67, 88], В.Г. Радзиевского [89-91], А.И. Рембовского, А.В. Ашихмина, В.А. Козьмина [101], Ю.К. Меньшакова [102, 103] изложены в общем виде основы организации радиомониторинга, требования к трактам специального приема и принципы размещения средств радиомониторинга на местности.

В качестве примера первого направления исследований можно привести работу [202], в которой представлен подход к техническому анализу и обработке сложных информационных сигналов современных цифровых систем передачи информации как многоэтапный процесс, организация которого требует рассмотрения и учета многих факторов. Показано, что технический анализ сигналов систем связи для вскрытия процедуры преобразования данных делится на уровни структурной иерархии, определяемые структурой и параметрами преобразований сигнала, в процессе оптимизации цифровых

потоков. Технический анализ сигналов для вскрытия процедуры преобразования данных в условиях структурной и параметрической неопределенности процедур представления сообщений основывается на совокупности информативных признаков, которые соответствуют структуре обрабатываемого сигнала. При этом целью является выявление этих информативных признаков путем аналитического описания процесса формирования исследуемого цифрового потока, которое может быть представлено в виде модели процедуры преобразования сигналов систем связи.

Этому же направлению исследований соответствуют работы П.А. Дятлова и Б.Х. Кульбикаяна [85, 86, 100], которые посвящены вопросам увеличения зоны энергетической доступности и достоверности радиомониторинга в условиях использования в системах радиосвязи, радиолокации и радионавигации различных режимов работы (например, режимы с низкоэнергетическими широкополосными сигналами), а также обеспечение контроля пространственных, энергетических, частотных и временных характеристик радиомониторинга спутниковых радионавигационных систем.

Работа Ю.А. Смирнова [194] является примером второго направления исследований в области радиомониторинга. В ней описаны пути рационального построения средств радиомониторинга в условиях различного значения параметров радиоэлектронных средств противника в целях информационного обеспечения боевой деятельности группировки в целом. Кроме того, предложена методика оценки эффективности системы радиомониторинга через коэффициент полноты отображения разведуемых объектов, как отношение числа разведанных объектов за некоторое время к общему числу объектов в зоне разведки.

Вместе с тем, следует отметить, что в имеющихся открытых работах недостаточно внимания уделено совершенствованию концептуальных основ ведения радиомониторинга в современных условиях перехода войск к сетецентрической системе управления. За пределами исследований остаются аспекты информационного конфликта между системами связи и радиомониторинга. Кроме того, в работах Ю.Л. Козирацкого [1, 98], В.И. Владимирова [60, 77] и В.В. Цветнова [66, 67], радиомониторинг рассматривается исключительно с позиции системы целенаведения для комплексов радиоэлетронного подавления (РЭП), при этом вопросы продолжительного во времени наблюдения за источниками радиоизлучений, а также обработки информации исследованы недостаточно глубоко.

Вместе с тем, как показано в работе М.И. Каратуева [131], сущность взаимодействия сил и средств разведки, РЭБ и огневого поражения должна заключаться в согласованном по задачам, месту и времени непрерывном действии сил и средств, ведущих разведку, осуществляющих сбор, обработку разведывательной информации и быстрое ее доведение до соответствующих органов (пунктов) управления войсками и оружием в целях принятия наиболее целесообразных решений при огневом поражении и радиоэлектронном

подавлении противника в операции. В качестве одного из направлений реализации такого взаимодействия автором обозначена необходимость комплексной автоматизации системы разведки в интересах огневого поражения противника. Указанная автоматизация должна предусматривать [131]:

- создание мобильных автоматизированных пунктов управления разведкой (прежде всего, командно-разведывательных центров из состава пунктов управления разведкой общевойсковых формирований, а также пунктов управления артиллерийской разведкой оперативного и тактического звеньев управления);
- размещение автоматизированных рабочих мест должностных лиц разведки на пунктах управления огневыми формированиями родов войск;
- оснащение всех сил и средств разведки, взаимодействующих с огневыми (ударными) формированиями, унифицированными техническими средствами управления и связи;
- автоматизацию основных процессов разведки (поиск, обнаружение, распознавание объектов и определение их координат) и управления ее силами и средствами.

В работе В.Ф. Комаровича и И.Б. Саенко [205] рассмотрена концепция компьютерной информационной войны и показано место радиомониторинга как оборонительного средства для предотвращения и обнаружения информационных действий противника, а также организации контрдействий.

Работа А. Ильина и Н. Шакина [206] указывает на недопустимость раздельного рассмотрения различных аспектов радиомониторинга, радиоэлектронной борьбы и радиоэлектронной маскировки, без их взаимосвязи в рамках единой системы информационной борьбы в военной сфере, без должного анализа этих категорий военной науки и практики как составных частей общей военно-научной области – борьбы в информационной сфере. По мнению авторов, такой анализ необходим как с научно-методологической (теоретической), так и с практической (организационной) точек зрения. С теоретической точки зрения радиомониторинг, радиоэлектронная борьба и радиоэлектронная маскировка, будучи составляющими (подсистемами) информационной борьбы, обладают как общими системными свойствами (признаками) целого, так и специфическими особенностями, которые определяют содержание рассматриваемых компонентов. В практическом плане общие (совпадающие) области и мероприятия радиомониторинга, радиоэлектронной борьбы и радиоэлектронной маскировки требуют, с одной стороны, однозначного толкования и организационного объединения, а с другой – более четкого разграничения. Это утверждение относится, прежде всего, к целям, задачам и принципам рассматриваемых радиоэлектронно-информационных составляющих информационной борьбы в военной сфере.

Таким образом, радиомониторинг, являясь организационно-технической основой специальной работы вообще, своей основной целью имеет обеспечение органов управления во главе с лицом, принимающим решение, необходимой

информацией о противнике. К наступательной стороне радиомониторинга относится добывание информации о противнике, а к оборонительной – радиоэлектронная защита своих средств радиомониторинга, в том числе и меры по скрытию ведения специальной работы. Радиомониторинг, обеспечивая достоверной информацией лиц, принимающих решения, создает условия для принятия обоснованных решений по управлению своими войсками (силами) и оружием. Этим радиомониторинг вносит свой вклад в повышение эффективности управления, в том числе и в увеличение эффективности радиоэлектронного поражения радиоэлектронных объектов противника и радиоэлектронной защиты своих радиоэлектронных объектов. Вместе с тем, в настоящее время система радиомониторинга является пассивной, т.е. ее эффективность зависит от способности функционировать в условиях, определяемых режимами работы систем связи противоборствующей стороны. В связи с этим, перспективным направлением является разработка активных методов радиомониторинга, предполагающих осуществление тестовых деструктивных воздействий на системы связи (в первую очередь, в рамках совместного использования средств радиомониторинга со средствами РЭП) в целях приведения ее в состояние, характеризующееся требуемым уровнем разведдоступности.

Информационный конфликт систем связи в условиях радиоэлектронной борьбы и информационного противоборства

Информационный конфликт между системами радиоэлектронного подавления и системой радиосвязи широко исследован в работах А.Г. Зюко [116], В.И. Коржика, М.М. Финка, К.Н. Щелкунова [117], А.И. Палия [65], Г.И. Тузова [118], М.В. Максимова [63], Ю.М. Перунова, В.В. Мацукевича, А.А. Васильева [72], В.И. Владимирова [60, 77, 121-125], В.И. Борисова, В.М. Зинчука [119, 120], А.Е. Лимарева, А.В. Немчилова, А.А. Чаплыгина [120], В.Г. Радзиевского [74], А.И. Куприянова [68, 69], Л.Н. Шустова [69], А.В. Сахарова [68], М.А. Семисошенко [126], А.М. Чуднова [127-129, 368], П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко [129], Д.Л. Бураченко [130], В.И. Кузнецова [132], А.В. Боговика, В.В. Игнатова [133], Е.Е. Исакова [134], С.М. Одоевского, В.И. Калюки [135], В.И. Николаева, А.Е. Фёдорова [136, 137], Е.А. Шабалина [138, 139], Н.М. Радько, А.Н. Мокроусова [140], Г.Н. Мальцева, В.В. Вознюка, М.Р. Туктамышева [141], М.И. Жодзишского [369], T. Bazar [370], C. Cahn [371], Д.Г. Козлова [378], А.Н. Путилина [379-381]. 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 Ю.И. Стародубцева, В.В. Бухарина, С.С. Семенова [157-160] в настоящее время наблюдается расширение сферы ведения информационного конфликта применительно к системам связи и выход его за пределы 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. Данные аспекты исследованы в работах Л.О. Мыровой [207, 272], А.З. Чепиженко [207], В.Д. Добыкина, А.И. Куприянова, В.Г. Пономарева, Л.Н. Шустова [208], Б.Б. Акбашева, Н.В. Балюка, Л.Н. Кечиева [209], Р.М. Гизатуллина, З.М. Гизатуллина [210], А.В. Царегородцева [270-272], В.А. Михайлова [211, 273], О.В. Михеева [212], Н.С. Хохлова, А.В. Сидорова [213, 214], С.П. Якушина [215], А.А. Привалова [229, 230], а также в работах других ученых. 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.

Имеется большое количество работ по моделированию воздействия ИТВ на системы связи на канальном, сетевом и транспортном уровнях OSI (Open System Interconnection Reference Model), а также моделированию влияния эффектов от таких воздействий на информационно-управляющие системы, в составе которых функционирует система связи. Так, к таким работам можно отнести исследования: П.Н. Девянина [112], С.М. Климова [216, 217], А.И. Куприянова, А.В. Сахарова, В.А. Шевцова [108], О.И. Шелухина [165], А.В. Аграновского, Р.А. Хади, М.Б. Якубца [224, 225], А.А. Малюка [226], Ю.И. Стародубцева, В.В. Бухарина, С.С. Семенова, А.В. Кирьянова [157-160], Е.В. Гречишникова [275-278], П.Д. Зегжды, Д.П. Зегжды [282, 283, 284], А.А. Молдовяна [267], И.В. Котенко, И.Б. Саенко [248, 279-281], В.И. Емелина [172], М.А. Коцынюка, О.С. Лауты [166, 167], Г.А. Остапенко [218-220, 363-366], А.О. Калашникова, М.В. Бурсы [218-220], Д.Г. Плотникова, Ю.Н. Гузева [363-366], Н.М. Радько, И.О. Скобелева [221], Ю.К. Язова [222], А.С. Пахомовой [113, 144], И.И. Чукляева, А.В. Морозова [110, 155, 156], А.Б. Исупова [227, 228], А.А. Тарасова [243], С.Н. Новикова [258], А.С. Маркова [267], А.В. Царегородцева [269], и других ученых. 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: Д.А. Новикова [19, 20, 22], С.П. Расторгуева, М.В. Литвиненко [50], А.Г. Ломако, Д.Н. Бирюкова [149-151, 153], И.Е. Горбачева [175], Г.Н. Мальцева [147, 148], Г.А. Остапенко [168, 169], С.Н. Гриняева [234], В.В. Прилепского [235], Н.Н. Толстых [51, 142, 181, 182, 251, 252, 268], А.Н. Асоскова, И.Н. Малышевой [52], Л.Е. Мистрова [239, 240], Ю.Л. Козирацкого [1, 98, 241, 242], С.А. Будникова [1, 144, 244-246], А.А. Бойко [145, 233, 246, 247], В.Ю. Храмова [247], А.А. Сироты [249, 250], М.А. Стюгина [253-256], В.А. Шевцова [257], И.И. Чукляева [154], С.А. Якушенко [259], А.В. Данаева, А.А. Воробьева [260], И.В. Котенко [248, 281, 340-342], И.Б. Саенко [248, 281], А.В. Уланова [340-342] 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 Д.А. Новикова [187, 188] В.И. Владимирова [60], Ю.Л. Козирацкого [1, 61], В.Г. Радзиевского, А.А. Сироты [89], В.Р. Григорьева, Л.О. Шуркина [261] отмечается, что информационный конфликт между информационно-техническими системами, как правило, носит сложный иерархический характер и может состоять из множества дуэльно-игровых ситуаций на различных уровнях иерархии таких информационных систем.

В настоящее время имеется небольшое количество исследований по рассмотрению информационного конфликта в системах радиосвязи с учетом его развития на уровнях модели OSI выше физического, а также оценки вклада качества функционирования системы связи в эффективность системы управления. Эти исследования представлены в работах В.И. Владимирова [60, 121], С.И. Бабусенко, В.В. Исаева [264-266], А.М. Чуднова, П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко [129], А.В. Боговика, В.В. Игнатова [133], С.М. Одоевского, В.И. Калюки [135], а также в ранее опубликованных работах авторов – Макаренко С.И. и Михайлова Р.Л. [54, 285].

Вместе с тем имеется достаточное количество работ, посвященных исследованию изменения параметров систем радиосвязи на канальном уровне, и, прежде всего, эффектов снижения эффективности функционирования протоколов множественного доступа в сетях радиосвязи. К этим исследованиям можно отнести работы: В.И. Владимирова [77, 125], М.А. Семисошенко [126], Д.Л. Бураченко [130], А.А. Бойко [233], В.А. Вавилова, А.А. Назарова [286], В.М. Вишневского, А.И. Ляхова [287], М.Е. Елесина, Д.Н. Ходаревского [288], Д.А. Ковалькова [289], Д.С. Осипова [290], Е.А. Спириной [291], В.Р. Чакрян [292], Е.А. Шабалина [139, 139], С.И. Макаренко [273, 274], А.Н. Путилина [379-381], а также работы других авторов.

Имеются исследования влияния преднамеренных помех на сеть связи на сетевом и транспортном уровнях. В частности исследовались: топологические изменения, снижение структурной живучести и надежности сети связи, эффектов перемаршрутизации и обеспечения качества обслуживания информационных потоков в ней под влиянием внешних деструктивных факторов и преднамеренных помех. К таким исследованиям можно отнести работы: В.В. Поповского [293-295], А.В. Лемешко [295-297], А.А. Романюка [297], В.К. Попкова [298, 299], В.П. Блукке [299], А.А. Сорокина, В.Н. Дмитриева [300, 301], Д.А. Перепелкина [302-305], В.П. Корячко [305], В.И. Мейкшана [306], И.И. Пасечникова [307, 308], Ю.Ю. Громова [309], Д.А. Ковалькова [310], И.Э. Горбунов [311], М.М. Егунова, В.П. Шувалова [312], М.М. Ластовченко, Е.А. Зубарева, В.О. Саченко [313], А.В. Стромова, Ю.Б. Нечаева, А.Д. Баева [314], В.А. Цимбала, В.Е. Тоискина, И.А. Якимовой [315, 316], Свинцова А.А., Солодухи Р.А. [317], С.Е. Ададурова [231, 232], В.А. Михайлова [211, 273], Л.О. Мыровой [207, 272], А. В. Царегородцева [270-

272], Б.Б. Акбашева, Н.В. Балюка, Л.Н. Кечиева [209], Е.В. Гречишникова [277, 278], Г.А. Остапенко, Д.Г. Плотникова, Ю.Н. Гузева [363-366], а также более ранние работы авторов – С.И. Макаренко и Р.Л. Михайлова [285, 318-323].

Необходимо отметить, что в работах В.В. Поповского [293-295], А.В. Лемешко [295-297], А.А. Романюка [297], В.К. Попкова [298], В.П. Блукке [299], А.А. Сорокина, В.Н. Дмитриева [300, 301], Д.А. Перепелкина [302-305], В.П. Корячко [305], В.И. Мейкшана [306], И.И. Пасечникова [307, 308], Ю.Ю. Громова [309], Д.А. Ковалькова [310], И.Э. Горбунова [311], М.М. Егунова, В.П. Шувалова [312] рассматриваются вопросы влияния воздействия деструктивных факторов на динамическое изменение топологии сети, а также на отдельные процессы сетевого уровня. Однако в данных работах не учитывались специфика сетей специальной (военной) связи, а также особенности поражения их элементов преднамеренными деструктивными воздействиями.

В работах А.М. Чуднова, П.Н. Барашкова, А.П. Родимова, К.А. Ткаченко [129], А.В. Боговика, В.В. Игнатова [133], В.К. Попкова, В.П. Блукке [299], М.М. Ластовченко, Е.А. Зубарева, В.О. Саченко [313], А.В. Стромова, Ю.Б. Нечаева, А.Д. Баева [314], В.А. Цимбала, В.Е. Тоискина, И.А. Якимовой [315, 316], А.А. Свинцова, Р.А. Солодухи [317], которые посвящены устойчивости сетей специальной связи, не рассматриваются особенности процессов маршрутизации в сетях с переменной топологией. В работах С.Е. Ададурова [231, 232] – подробно рассматриваются процессы маршрутизации, частично рассматриваются эффекты от воздействия средств РЭП, однако не учитываются временные показатели процессов маршрутизации при таком воздействии на сеть. В работах В.А. Цимбала, В.Е. Тоискина, И.А. Якимовой [315, 316] рассматривается вопрос влияния помех на эффективность на функционирование протоколов обеспечения качества обслуживания, на примере протокола TCP. Однако, в этих работах помехи рассматривается как некоторый постоянно действующий фактор, а не как адаптивное воздействие, реализованное в виде соответствующего ИТВ, целью которого является снижение скорости соединений в сети.

В работах В.А. Михайлова [211, 273], Л.О. Мыровой [207, 272], А. В. Царегородцева [270-272], Б.Б. Акбашева, Н.В. Балюка, Л.Н. Кечиева [209], Е.В. Гречишникова [277, 278] исследовались вопросы воздействия электромагнитного излучения (мощного СВЧ излучения, а также сверхкоротких электромагнитных импульсов) на функционирование оборудования телекоммуникационных систем. Однако в них не рассматривались вопросы влияния данных средств на структуру информационных потоков, а также влияние эффектов такого воздействия на функционирование протоколов канального, сетевого и транспортного уровней модели OSI.

В последнее время активно ведутся исследования в области развития как средств РЭП и ИТВ, так и способов защиты от их применения по отношению к элементам систем специальной связи. К таким исследованиям можно отнести

работы: О.И. Шелухина [165], Ю.И. Стародубцева, В.В. Бухарина, С.С. Семенова, А.В. Кирьянова [157-160], Е.В. Гречишникова [275-278], П.Д. Зегжды, Д.П. Зегжды [282, 283, 284], И.В. Котенко, И.Б. Саенко [248, 279-281], М.А. Коцынюка, О.С. Лауты [166, 167], Г.А. Остапенко, А.О. Калашникова, М.В. Бурсы [219, 220], Н.М. Радько, И.О. Скобелева [221], А.Б. Исупова [227, 228], А.А. Тарасова [243], С.Н. Новикова [258], и других ученых. Воздействие ИТВ, как правило, ориентировано на деградацию процессов информационного обмена в узлах связи, прекращение доступа к услугам связи и разрушение информационных потоков. Таким образом, описание эффектов такого воздействия связано с процессами обработки информационных потоков в узлах связи, с вопросами изменения структуры информационных потоков, с появлением свойств нестационарности и особенностями их дальнейшей обработки, с функциональной и структурной деградацией сети вследствие ограниченной доступности ее ресурсов.

В настоящее время основу передаваемых информационных потоков составляет пакетный трафик, при этом особенности функционирования пакетных сетей связи широко исследуются методами теории телетрафика. Однако в исследованиях, основанных на теории телетрафика, свойства информационных потоков, влияющие на устойчивость системы связи, а также ограниченная надежность элементов системы рассматриваются как исходные условия, а не как эффект от целенаправленного деструктивного воздействия. Вместе с тем, в ограниченном количестве работ (в частности в работах О.И. Шелухина [165], Н.Н. Толстых [324], С.И. Макаренко [325], К.В. Ушанева [326]) рассматривается влияние свойств передаваемых информационных потоков (их самоподобные свойства, уровень сложности структуры, безопасность и др.) на устойчивость и безопасность системы связи в целом. При этом преднамеренное ухудшение свойств передаваемого трафика рассматривается как эффект, возникающий вследствие специализированных ИТВ на телекоммуникационные системы. Наличие таких деструктивных эффектов, а также необходимость противодействия им, позволяют сформулировать актуальную задачу моделирования информационного конфликта транспортного уровня OSI – между системой обеспечения заданного качества обслуживания трафика и системой ИТВ, ориентированной на его направленное деструктивное изменение свойств трафика. Причем данный конфликт может быть рассмотрен как конфликт наблюдения, когда по оценке изменения структурных свойств трафика определяется факт ИТВ, так и в качестве конфликта подавления – когда ведется изменение структурных свойств трафика, происходит подмена или внедрение пакетов, или ведется направление специально сгенерированных потоков трафика на отдельные узлы (DDOS и DOS атаки).

Таким образом, анализ известных работ показал, что рассмотрение процесса подавления линий и сетей связи ведется, как правило, без учета комплексного воздействия множества деструктивных факторов на процессы передачи информационных потоков, а также на их структуру. В известных

работах отсутствуют системные исследования эффектов от преднамеренных деструктивных воздействий (средств РЭП, средств ЭМИ и ИТВ) с учетом их межуровневого отображения на вышестоящие уровни модели OSI. Не учитывается влияние преднамеренных деструктивных воздействий на процессы маршрутизации информационных потоков в распределенных сетях, а также в сетях с динамически изменяемой топологией. Как правило, не рассматриваются вопросы обеспечения заданного качества обслуживания в распределенных сетях, находящихся под воздействием территориально-распределенной группировки средств деструктивных воздействий. И самое главное – в данных работах процесс воздействия рассматривается как некий постоянно действующий деструктивный фактор, а не как конфликтное взаимодействие с учетом адаптивной реакции участников в процессе развития информационного конфликта.

Таким образом, можно констатировать, что анализ исследований в области информационного конфликта в рамках РЭБ, а также в области информационного противоборства и информационной безопасности показал – требуется расширение понятия «*информационный конфликт*» на всю область информационного противоборства в технической сфере с включением в него уже разработанной методологии по конфликтам в области радиосвязи. При этом необходимо учесть, что объектами исследования теории информационного противоборства являются сложные многоуровневые иерархические информационно-управляющие метасистемы (государственные, политические, военные, социальные и экономические).

Как показано в работах Ю.И. Стародубцева [157-160], С.А. Будникова [244, 246], А.А. Бойко [246, 247], П.И. Антоновича [327], А.В. Паршуткина [262, 263], И.И. Чукляева [328] методология развития информационного противоборства в технической сфере связанна с комплексной интеграцией «классических» средств РЭП и новых способов ИТВ.

В известных работах по конфликтам в области информационного противоборства Д.А. Новикова [19, 20, 22], С.П. Расторгуева, М.В. Литвиненко [50], А.Г. Ломако, Д.Н. Бирюкова [149-151], Ю.Л. Козирацкого [98, 241], С.А. Будникова [244, 246], Г.А. Остапенко [168, 169, 363-366], Д.Г. Плотникова, Ю.Н. Гузева [363-366], как правило, основной упор делается на особенности стратегий участников. При этом в работах по информационному конфликту систем связи отсутствует его согласование с многоуровневой моделью OSI.

Имеются работы в области анализа функционирования комплексов связи и управления как многоуровневых иерархических систем А.М. Чуднова [129], И.М. Гуревича [329-332], А.А. Вакуленко, В.И. Шевчука [333], Ю.И. Маевского [334], В.В. Поповского, А.В. Лемешко, О.Ю. Евсеевой [335]. Однако за исключением работ А.М. Чуднова [129] и Ю.И. Маевского [334], в остальных работах не рассматриваются конфликтные ситуации, характерные для многоуровневого информационного конфликта. Очень интересной, в плане учета фактора многоуровневости конфликта, является работа Е.М. Воронова [59]. Она посвящена конфликтам в другой сфере – в области многообъектовой

противовоздушной обороны, и в ней рассмотрен многообъектный многоуровневый конфликт систем. Однако данная работа лишь в самых общих теоретических аспектах применима к описанию многоуровневого конфликта систем связи.

В работах А.В. Паршуткина [262, 263] представлено развитие модели информационного конфликта «классического» РЭП и систем радиосвязи в направлении повышения «многоуровнивости» 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. Таким образом, предложенный в работах А.В. Паршуткина [262, 263] новый концептуальный подход к моделированию информационного конфликта, с одной стороны органично развивает существующие работы в области многоуровневого информационного конфликта радиоэлектронных систем [1, 60, 89], 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 рамках модели CSI средствами вскрытия и наблюдения протоколов, используемых в системах связи, останутся «классические» средства радио- и компьютерной разведки, а средствами подавления – как «традиционные» средства РЭП, так и новые виды ИТВ.

В дальнейшем, в работе С.И. Макаренко [54] в качестве конкретизации модели CSI была предложена модель динамического конфликта многоуровневых сложных систем – системы связи и системы воздействия. Дальнейшее развитие этой модели возможно за счет формализации конфликтного взаимодействия на основе соответствующего научно-методического аппарата и внесение в модель формальных положений, описывающих многоуровневый конфликт. При этом надо отметить, что научно-методический аппарат для формализации информационного конфликта в наибольшей мере и наиболее полно разработан на основе:

- теории марковских процессов – воронежская научная школа, представленная работами: Ю.Л. Козирацкого, С.А. Будникова [1], В.И. Владимирова [60, 77, 121, 125], В.И. Борисова, В.М. Зинчука [119, 120], В.Г. Радзиевского [74, 89, 90], А.А. Сироты [89, 90], А.А. Бойко [146];
- теории игр – научная школа Военной академии связи, представленная работами: А.М. Чуднова [127-129], С.М. Одоевского, В.И. Калюки [135], М.А. Семисошенко [126], С.А. Якушенко [259], Д.Г. Козлова [378], А.Н. Путилина [379-381].

Вместе с тем, направление формализации информационного конфликта на основе теории динамических систем разработано недостаточно глубоко.

Развитие существующих работ в направлении учета многоуровневости системы связи в соответствии с моделью OSI, а также с учетом возможности комплексных многоуровневых деструктивных воздействий (обобщающих воздействие средств РЭП, средств ЭМИ и ИТВ на различных уровнях OSI) позволит сформировать научное направление исследования многоуровневых динамических информационных конфликтов. В рамках этого направления возможно исследовать нестационарные и динамические процессы протекания конфликта, а также его движение в пространстве состояний. Потенциально интересным развитием данного направления может стать проработка процессов поведения динамических моделей информационного конфликта в нестационарных и неустойчивых режимах, а в дальнейшем – переход к исследованию динамических моделей информационного конфликта на основе теории бифуркации, теории катастроф и теории детерминированного хаоса.

К отдельным работам, в которых уже сейчас просматривается данное актуальное направление исследований информационного конфликта, можно отнести работы Н.Н. Толстых [51, 251, 252, 268], И.И. Семеновой [336], Г.А. Остапенко, Д.Г. Плотникова, Ю.Н. Гузева [363-366], которые формализуют информационный конфликт на основе теории динамических систем, а также работы А.А. Колесникова [337, 338], в которых показана возможность формализации информационного конфликта на основе теории детерминированного хаоса, и даже управление конфликтом на основе методов этой теории. Кроме того, к работам, которые формализуют конфликты как динамические системы, традиционно относят исследования в области анализа биологических популяций (например, работа А.Д. Базыкина [339]).

Разработка моделей информационных конфликтов на основе теории динамических систем, теории бифуркации, теории катастроф и теории детерминированного хаоса позволит не только обогатить теорию информационного конфликта применительно к техническим системам, но и предложить принципиально новый научно-методический аппарат моделирования информационного конфликта для систем в политической, экономической и социальной сферах.

Заключение

Анализ известных работ в области информационного конфликта показал, что перспективным развитием методологии его исследования является:

- учет того, что прикладная область ведения информационного конфликта смещается в сторону единого информационно-телекоммуникационного пространства, которое является основой сетецентрического управления силами и средствами на всех этапах ведения боевых действий;
- учет сложности и многоуровневости конфликтующих систем, а также процессов межуровневого отображения отдельных воздействий внутри системы;

- учет взаимовлияния и разработка эффективных методов координации между отдельными подсистемами внутри конфликтующих систем (например таких, как подсистема радиомониторинга и подсистема РЭП в метаконфликте «система связи»–«система воздействий»);
- учет новых видов конфликтов, типа «скрытый конфликт», связанных с воздействиями, ориентированными на порождение или развитие внутренних противоречий в конфликтующей системе, навязывание ложных целей, перехват управления, нарушение координации и др.;
- учет возможности участия в информационном конфликте более двух сторон, с возможностью таких отношений между участниками как сотрудничество, симбиоз, нейтралитет и др.;
- учет динамических свойств информационного конфликта за счет его формализации на основе теории динамических систем, теории бифуркации, теории катастроф и теории детерминированного хаоса;
- развитие известного и в достаточной мере разработанного научно-методического аппарата исследования информационного конфликта для моделирования конфликтов информационных систем в политической, экономической и социальной сферах.

Применительно к информационному конфликту наблюдения в прикладной области мониторинга перспективным развитием методологии его исследования является:

- смещение процессов конфликта наблюдения в область единого информационно-технического пространства, в котором всю большую роль будут играют методы компьютерной разведки, методы добывания информации из открытых источников, методы анализа Big Date;
- учет того, что в конфликте «система связи» – «система воздействий», система воздействий является сложной системой, включающей в себя две подсистемы, с различными (ограниченно антагонистическими) целями функционирования – подсистему подавления и подсистему мониторинга. Различность целей этих подсистем делают актуальной задачу координации их функционирования в интересах максимизации выигрыша «системы воздействий», при ограничениях на доступные ее подсистемам общий ресурс, и их локальные стратегии;
- учет иерархичности конфликтующих систем и различного уровня их наблюдаемости на различных иерархиях конфликтующих систем, согласования уровней конфликта наблюдения с уровнями модели OSI;
- учет новых видов конфликтов, типа «скрытый конфликт», связанного с формированием ложного канала наблюдения, внесениями в канал наблюдения искажений, направленных на формирование ложного видения обстановки, или на формирование фрагментарного восприятия, без виденья общей цельной картины наблюдения в конфликте систем;

- учет динамических свойств конфликта наблюдения и его динамической взаимосвязи с метаконфликтом систем на более высоком уровне.

Применительно к информационному конфликту подавления в прикладной области систем связи перспективным развитием методологии его исследования является:

- смешение процессов конфликта подавления в область единого информационно-технического пространства, в котором всю большую роль будут играть комплексы воздействия, включающие в себя как РЭП, воздействующие на нижние уровни, так и ИТВ, воздействующие на верхние уровни функционирования системы связи;
- учет сложности и многоуровневости систем связи и согласование конфликта с многоуровневой моделью OSI, а также учетом процессов межуровневого отображения воздействий внутри системы связи через функциональные связи между ее отдельными протоколами;
- учет новых видов конфликтов, типа «скрытый конфликт», связанного с такими воздействиями на систему связи, которые ориентированны на порождение или развитие внутренних противоречий между ее протоколами, навязывание неверного управления ими, или перехват управления отдельными элементами системы;
- учет динамических свойств информационного конфликта за счет его формализации на основе теории динамических систем, теории бифуркации, теории катастроф и теории детерминированного хаоса.

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. Козирацкого Ю.Л. – М.: Радиотехника, 2013. – 232 с.

2. Гаврилов В. М. Оптимальные процессы в конфликтных ситуациях. – М: Сов. радио, 1969. – 160 с.

3. Крапивин В. Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях. – М.: Сов. радио, 1972. – 192 с.

4. Лефевр В. А. Конфликтующие структуры. – М.: Сов. радио, 1973. – 159 с.

5. Саати Т. Л. Математические модели конфликтных ситуаций / Пер. с англ. Под ред. И. А. Ушакова. – М.: Сов. Радио, 1977. – 170 с.

6. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 344 с.

7. Месарович М., Такахара И. Общая теория систем. Математические основы. – М., 1978. – 311 с.

8. Данилов Н. Н. Игровые модели принятия решений. – Кемерово, 1981. 122 с.

9. Берзин Е. Л. Оптимальное распределение ресурсов и теория игр / Под ред. Золотова Е. В. – М.: Радио и связь, 1983. – 216 с.

10. Кукушкин Н. С., Меньшикова О. Р., Меньшиков И. С. Конфликты и компромиссы. – М.: Знание, 1986. – 32 с.

11. Горелик В. А., Кононенко А. Ф. Теоретико-игровые модели принятия решений в эколого-экономических системах. – М.: Радио и связь, 1982. – 144 с.

12. Горелик В. А., Горелов М. А., Кононенко А. Ф. Анализ конфликтных ситуаций в системах управления. – М.: Радио и связь, 1991. – 288 с.

13. Чикрий А. А. Конфликтно-управляемые процессы. – Киев: Наукова думка, 1992. – 383 с.

14. Бурков В. Н., Данаев Б., Еналиев А. К., Кондратьев В. В., Нанева Т. Б., Шепкин А. В. Большие системы: моделирование организационных механизмов. – М.: Наука, 1989. – 246 с.

15. Бурков В. Н., Ириков В. А. Модели и методы управления организационными системами. – М.: Наука, 1994. – 270 с.

16. Малафеев О. А., Муравьев А. И. Математические модели конфликтных ситуаций и их разрешение. Т. 1. Общая теория и вспомогательные сведения. – СПб.: СПб гос. ун-т экон. и финансов, 2000. – 283 с.

17. Светлов В. А. Аналитика конфликта. Учебное пособие. – СПб.: Росток, 2001. – 511 с.

18. Новосельцев В. И. Системная конфликтология. – Воронеж: Кварта, 2001. – 169 с.

19. Новиков Д. А., Чхартишвили А. Г. Рефлексивные игры. – М.: СИНТЕГ, 2003. – 149 с.

20. Новиков Д. А., Чхартишвили А. Г. Прикладные модели информационного управления. – М.: ИПУ РАН, 2004. – 129 с.

21. Новиков Д. А. Теория управления организационными системами. 2-е изд. – М.: Физматлит, 2007. – 584 с.

22. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. – М.: Физматлит, 2010. – 244 с.

23. Мистров Л. Е., Сербулов Ю. С. Методологические основы синтеза информационно-обеспечивающих функциональных организационно-технических систем. – Воронеж: Научная книга, 2007. – 232 с.

24. Мистров Л. Е. Моделирование информационных структур обеспечения конфликтной устойчивости взаимодействия организационно-технических систем. Дис. ... д-ра техн. наук. – Тамбов, 2008. – 435 с.

25. Сербулов Ю. С. Модели выбора и распределения ресурсов технологических систем в условиях их замещения и конфликта. Дис. … д-ра техн. наук. – Воронеж, 1999. – 306 с.

26. Величко С. В., Мистров Л. Е., Сербулов Ю. С. Методологические основы синтеза решений по управлению экологическими конфликтами. – Воронеж: Научная книга, 2008. – 386 с.

27. Угольницкий Г. А. Иерархическое управление устойчивым развитием. – М.: Издательство физико-математической литературы, 2010. – 336 с.

28. Угольницкий Г. А., Усов А. Б. Устойчивое развитие систем управления в условиях коррупции // Математическая теория игр и ее приложения. 2010. Т. 2. № 4. С. 106-119.

29. Угольницкий Г. А., Усов А. Б. Вертикальные коалиции в иерархических трехуровневых системах управления веерной структуры // Известия Российской академии наук. Теория и системы управления. 2010. № 6. С. 94-101.

30. Усов А. Б. Борьба с коррупцией в динамических системах управления иерархической структуры // Известия Южного федерального университета. Технические науки. 2012. № 6 (131). С. 224-228.

31. Деттмер У. Теория ограничений Голдратта: Системный подход к непрерывному совершенствованию. Пер. с англ. 2-е изд. – М.: Альпина Бизнес Букс, 2008. – 444 с.

32. Алгазин Г. И. Эколого-экономические с различной информированностью участников: модели, механизмы функционирования, оценки эффективности. – Барнаул: АлтГУ, 1997.

33. Алгазин Г. И. Модели системного компромисса в социально-экономических исследованиях: монография. – Барнаул: Азбука, 2009. – 239 с.

34. Алгазин Г. И. Методологические аспекты математического исследования конфликтов в современных теориях организационных систем // Известия Алтайского государственного университета. 2001. № 1. С. 7-9.

35. Жуковский В. И., Кудрявцев К. Н. Уравновешивание конфликтов и приложения. – М.: УРСС, 2012. – 304 с.

36. Жуковский В. И., Жуковская Л. В. Риск в многокритериальных и конфликтных системах при неопределенности. Монография. – М.: УРСС, 2004. – 267 с.

37. Сысоев Д. В. Условия формирования конфликта в приведенных системах // Научный вестник Воронежского государственного архитектурно-строительного университета. Серия: Информационные технологии в строительных, социальных и экономических системах. 2013. № 1. С. 41-48.

38. Сысоев В. В., Сысоев Д. В. Действие системы // Системы управления и информационные технологии. 2005. № 1 (18). С. 51-58.

39. Сысоев В. В. Определение конфликта функционирующих систем // Математическое моделирование технологических систем. Сб. науч. тр. – Воронеж: Воронеж. гос. технол. акад. 1996. – С. 3-9.

40. Сысоев В. В. Конфликт. Сотрудничество. Независимость. Системное взаимодействие в структурно-параметрическом представлении. – М.: Моск. акад. экон. и права, 1999. – 151 с.

41. Сысоев В. В. Моделирование структуры конфликта функционирующих систем // Информационные технологии и системы. Тез. докл. Всерос. конф. – Воронеж: Воронеж. гос. технол. акад, 1995. – С. 6-7.

42. Рубинштейн М. И. Оптимальная группировка взаимосвязанных объектов. – М.: Наука, 1989. – 168 с.

43. Корягин М. Е. Оптимизация управления городскими пассажирскими перевозками на основе конфликтно-устойчивых решений. Диссертация … докт. техн. наук – Новокузнецк: Кузбасский государственный технический университет. 2011. – 345 с.

44. Корягин М. Е. Равновесные модели системы городского пассажирского транспорта в условиях конфликта интересов. – Новосибирск: Наука, 2011. – 140 с.

45. Гурин Л. С., Дымарский Я. С., Меркулов А. Д. Задачи и методы оптимального распределения ресурсов. – М.: Сов. радио, 1968. – 463 с.

46. Гусейнов Б. А., Ушаков И. А. Оптимальное распределение ресурсов в территориальных системах. – М.: ВЦ АН СССР, 1985. – 52 с.

47. Мистров Л. Е. Основы методологии организационно-функционального синтеза сложных систем // Приборы и системы. Управление, контроль, диагностика. 2006. № 12. С. 56-61.

48. Мистров Л. Е. Метод аналитического решения задачи системотехнического синтеза конфликтно-устойчивых обеспечивающих функциональных организационно-технических систем // Машиностроитель. 2005. № 1. С. 25-33.

49. Бухарин С. Н., Цыганов В. В. Методы и технологии информационных войн. – М.: Академический Проект, 2007. – 382 с.

50. Расторгуев С. П., Литвиненко М. В. Информационные операции в сети Интернет / Под общ. ред. А.Б. Михайловского. – М.: АНО ЦСОиП, 2014. – 128 с.

51. Алферов А. Г., Белицкий А. М., Степанец Ю. А., Толстых Н. Н. Перехват управления инфокоммуникационных систем // Теория и техника радиосвязи. 2014. № 4. С. 5-13.

52. 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.

53. Никольский Б. А. Основы теории систем и комплексов радиоэлектронной борьбы: электрон. учеб. пособие. – Самара: Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т), 2012. – 174 с.

54. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122-185. – URL: http://journals.intelgr.com/sccs/archive/2015-03/07-Makarenko.pdf (дата обращения 03.04.2016).

55. Новиков Д. А. Иерархические модели военных действий // Управление большими системами. 2012. № 37. С. 25-62.

56. Ашкеназы В. О. Применение теории игр в военном деле. – М.: Советское радио, 1961. – 362 с.

57. Дружинин В. В., Конторов Д. С. Вопросы военной системотехники. –

М.: Воениздат, 1976. – 224 с.

58. Дружинин В. В., Конторов А. С., Конторов Д. С. Введение в теорию конфликта. – М.: Радио и связь, 1989. – 288 с.

59. Воронов Е. М. Методы оптимизации управления многообъектными многокритериальными системами на основе стабильно-эффективных игровых решений: Учебник / Под ред. Н.Д. Егупова. – М.: МГТУ им. Н.Э. Баумана, 2001. – 576 с.

60. Владимиров В. И., Владимиров И. В. Основы оценки конфликтно-устойчивых состояний организационно-технических систем (в информационных конфликтах). – Воронеж: ВАИУ, 2008. – 231 с.

61. 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.

62. Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. – М.: Сов. радио. 1968. – 448 с.

63. 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.

64. Дружинин В. В., Конторов Д. С. Конфликтная радиолокация. – М.: Радио и связь, 1982. – 288 с.

65. Палий А. И. Радиоэлектронная борьба. – М.: Воениздат, 1989. – 350 с.

66. Цветнов В. В., Демин В. П., Куприянов А. И. Радиоэлектронная борьба: радиоразведка и радиопротиводействие. – М.: МАИ, 1998. – 248 с.

67. Цветнов В. В., Демин В. П., Куприянов А. И. Радиоэлектронная борьба: радиомаскировка и помехозащита. – М.: МАИ, 1999. – 240 с.

68. Куприянов А. И., Сахаров А. В. Радиоэлектронные системы в информационном конфликте. – М.: Вузовская книга, 2003. – 528 с.

69. Куприянов А. И., Шустов Л. Н. Радиоэлектронная борьба. Основы теории. – М.: Вузовская книга, 2011. – 800 с.

70. Куприянов А. И. Радиоэлектронная борьба. – М.: Вузовская книга, 2013. – 360 с.

71. Перунов Ю. М., Фомичев К. И., Юдин Л. М. Радиоэлектронное подавление информационных каналов систем управления оружием / Под. ред. Ю.М. Перунова. – М.: Радиотехника, 2003. – 416 с.

72. 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.

73. Радзиевский В. Г. Метод обоснования характеристик сигнало-подобных излучений в конфликтной радиолокации // Радиотехника. 2000. № 6. С. 53-58.

74. Современная радиоэлектронная борьба. Вопросы методологии / Под ред. В.Г. Радзиевского. – М.: Радиотехника, 2006. – 424 с.

75. Сухоруков Ю. С., Шляхин В. М. Конфликтно-игровая модель радиолокационного обнаружения целей в условиях противодействия //

Радиоэлектроника. 1991. № 9. С. 44-59.

76. Сухоруков Ю. С, Шляхин В. М. Принципы моделирования динамики взаимодействия сторон в условиях радиолокационного конфликта // Радиотехника. 1992. № 1-2. С. 4-11.

77. Владимиров В. И., Лихачев В. П., Шляхин В. М. Антагонистический конфликт радиоэлектронных систем. – М.: Радиотехника, 2004. – 384 с.

78. Шляхин В. М., Каркоцкий В. Л., Яковлев Ю. В. Конфликтно-обусловленные выигрыши сторон в условиях противодействия // Радиотехника. 1992. № 7-8. С. 3-6.

79. Шляхин В. М., Яковлев Ю. В. Контррадиоподавление // Известия вузов. Радиоэлектроника. 2004. Т. 47. № 4. С. 3-13.

80. Меркулов В. И., Чернов В. С., Дрогалин В. В., Канащенков А. И., Самарин О. Ф., Алексеев Ю. Я., Громов М. В., Дудник П. И., Жибуртович Н. Ю., Ильчук А. Р., Родзивилов В. А., Слукин Т. П., Федоров И. Б., Францев В. В., Чернов М. В., Шуклин А. И. Помехозащищённость радиолокационных систем. Состояние и тенденции развития. / Под ред. А. И. Канащенкова, В. И. Меркулова. – М.: ИПРЖР, 2003. – 464 с.

81. Мельников Ю. П. Воздушная радиотехническая разведка (методы оценки эффективности). – М.: Радиотехника, 2005. – 304 с.

82. Миронов В. А., Радзиевский В. Г. Особенности навигационно-временного обеспечения радиоэлектронных систем в условиях конфликта // Радиотехника. 1998. № 6. С. 4-9.

83. Миронов В. А., Радзиевский В. Г. Помехозащищенность аппаратуры радиоинерциального навигационного комплекса с адаптивной антенной решеткой // Радиотехника. 1999. № 6. С. 79-82.

84 Миронов В. А. Методические основы исследования эффективности функционирования аппаратуры потребителей спутниковых систем навигационно-временного обеспечения в условиях радиоэлектронного конфликта // Радиотехника. 2010. № 6. С. 87-90.

85. Дятлов А. П., Кульбикаян Б. Х. Радиомониторинг излучений спутниковых радионавигационных систем. Монография. – М.: Радио и связь, 2006. – 270 с.

86. Дятлов А. П., Дятлов П. А., Кульбикаян Б. Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. Монография. – М.: Радио и связь, 2004. – 226 с.

87. Вартанесян В. А. Радиоэлектронная разведка. – М.: Воениздат, 1991. – 254 с.

88. Демин В. П., Куприянов А. И., Сахаров А. В. Радиоэлектронная разведка и радиомаскировка. – М.: МАИ, 1997. – 155 с.

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

90. Радзиевский В. Г., Сирота А. А. Теоретические основы радиоэлектронной разведки. 2-е изд. – М.: Радиотехника, 2004. – 432 с.

91. Радзиевский В. Г., Сирота А. А. Базовые статистические модели процесса радиотехнической разведки в ходе противодействия радиолокационным средствам // Радиотехника. 1992. № 1-2. С. 24-31.

92. Радзиевский В. Г., Сирота А. А. Особенности синтеза алгоритмов обработки информации при анализе состояния сложных радиоэлектронных объектов противодействия // Информационный конфликт в спектре электромагнитных волн (приложение к журналу Радиотехника). 1994. С. 4-13.

93. Сирота А. А., Борисов Ю. А. Алгоритмы фильтрации при поступлении ошибочных и противоречивых данных в каналах наблюдения систем сбора и обработки информации // Радиотехника. 1997. № 6. С. 51-57.

94. Сирота А. А. Вероятностные модели формирования результирующего вектора наблюдений в многоуровневых, многопозиционных системах // Радиотехника. 1998. № 6. С. 10-14.

95. Сирота А. А., Борисов Ю. А. Границы для точностных характеристик фильтров оценивания в условиях частичной скрытности наблюдаемых объектов // Синтез, передача и прием сигналов управления и связи (Межвузовский сборник научных трудов). 1997. № 4. С. 59-66.

96. Левашова Т. В. Принципы управления онтологиями, используемые в среде интеграции знаний // Труды СПИИРАН. 2002. Том 2. № 1. С. 51-68.

97. Дворников С. В. Теоретические основы частотно-временного анализа кратковременных сигналов. Монография. / Под ред. А.М. Кудрявцева. – СПб.: ВАС, 2010. – 240 с.

98. 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.

99. Леньшин А. В. Бортовые системы и комплексы радиоэлектронного подавления. – Воронеж: Научная книга, 2014. – 590 с.

100. Дятлов А. П., Кульбикаян Б. Х. Корреляционная обработка широкополосных сигналов в автоматизированных комплексах радиоконтроля. Монография. – М.: Горячая линия-телеком, 2013. – 332 с.

101. Рембовский А. И., Ашихмин А. В., Козьмин В. А. Радиомониторинг - задачи, методы, средства. 2-е изд. – М.: Горячая линия-Телеком, 2010. – 624 с.

102. Меньшаков Ю. К. Виды и средства иностранных технических разведок: учебное пособие / Под ред. М.П. Сычева. – М.: МГТУ им. Н.Э. Баумана, 2009. – 656 с.

103. Меньшаков Ю. К. Основы защиты от технических разведок: учебное пособие / Под ред. М.П. Сычева. – М.: МГТУ им. Н.Э. Баумана, 2011. – 487 с.

104. Лифанов Ю. С., Саблин В. Н., Салтан М. И. Направления развития зарубежных средств наблюдения над полем боя. – М.: Радиотехника, 2004. – 64 с.

105. Вакуленко А. А., Верба В. С., Дод В. Н. Организация конфликтно-устойчивого управления интегрированной радиоэлектронной системой в динамике конфликта со средствами радиоэлектронного подавления //

Радиотехника. 2006. № 1. С. 50-53.

106. Гребенюк В. Л., Исаев В. В., Мельников В. Ф. Оптимизация управления средствами радиопомех в трехстороннем конфликте со средствами радиоразведки и системой передачи информации // Информационно-измерительные и управляющие системы. 2009. Т. 7. № 9. С. 42-48.

107. Хореев А. А. Технические средства и способы промышленного шпионажа. – М.: ЗАО «Дальснаб», 1997. – 230 с.

108. Куприянов А. И., Сахаров А. В. Шевцов В. А. Основы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2006. – 256 с.

109. Аверченков В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т. Р. Методы и средства инженерно-технической защиты информации. Учебное пособие. – М.: ФЛИНТА, 2011. – 187 с.

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

111. Гольдштейн Б. С., Крюков Ю. С., Пинчук А. В., Хегай И. П., Шляпоберский В. Э. Интерфейсы СОРМ. Справочник. – СПб.: БХВ-Петербург, 2006. – 160 с.

112. Девянин П. Н. Модели безопасности компьютерных систем: учебное пособие для студентов вузов. – М.: Издательский центр «Академии», 2005. – 144 с.

113. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 115-118.

114. Бугров Ю. Г., Пахомова А. С., Бабурин А. В. Уточнение технологической схемы компьютерной разведки с учетом классификации компьютерных атак и возможностей вредоносных средств // Информация и безопасность. 2014. Т. 17. № 2. С. 292-295.

115. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. – СПб: ВМА, 2000. – 166 с.

116. Зюко А. Г. Помехоустойчивость и эффективность систем связи. – М.: Связь, 1972. – 359 с.

117. Коржик В. И., Финк М. М., Щелкунов К. Н. Расчет помехоустойчивости систем передачи дискретной информации. Справочник. – М.: Радио и связь, 1981. – 267 с.

118. 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.

119. Борисов В. И., Зинчук В. М. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. – М.: Радио и связь, 1999. – 252 с.

120. 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.

121. Владимиров В. И. Принципы и аппарат системных исследований радиоэлектронного конфликта. Учебное пособие. – Воронеж: ВВВИУРЭ, 1992.

122. Владимиров В. И., Гальянов Г. П. Эффективность комплексов РЭП и методы ее оценки. Учебное пособие. – Воронеж: ВВИУРЭ, 1993.

123. 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.

124. Владимиров В. И. Системы и комплексы РЭБ. Часть 1: Системотехнические основы построения. Курс лекций. – Воронеж: ВИРЭ, 1999.

125. Владимиров В. И. Информационные основы радиоподавления линий радиосвязи в динамике радиоэлектронного конфликта. – Воронеж: ВИРЭ, 2003. – 276 с.

126. Семисошенко М. А. Управление автоматизированными сетями декаметровой связи в условиях сложной радиоэлектронной обстановки. – СПб.: ВАС, 1997. – 364 с.

127. Чуднов А. М. Анализ помехозащищенности линий и сетей связи. – Л.: ВАС, 1988. – 34 с.

128. Чуднов А. М. Помехоустойчивость линий и сетей связи в условиях оптимизированных помех. – Л.: ВАС, 1986. – 84 с.

129. 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.

130. Бураченко Д. Л. Оптимальное разделение цифровых сигналов многих пользователей в линиях и сетях связи в условиях помех. – Л.: ВАС, 1990. – 302 с.

131. Каратуев М. И. Взаимодействие сил и средств разведки и огневого поражения в операции // Военная мысль. 1998. № 6 (11-12). С. 37-41.

132. Кузнецов В. И. Радиосвязь в условиях радиоэлектронной борьбы. – Воронеж: ВНИИС. 2002. – 403 с.

133. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.

134. Исаков Е. Е. Устойчивость военной связи в условиях информационного противоборства. – СПб.: Изд-во Политехн. ун-та, 2009. – 400 с.

135. 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.

136. 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.

137. 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.

138. Шабалин Е. А. Способы повышения эффективности систем радиосвязи в условиях конфликта // Электросвязь. 2008. № 9. С. 40-44.

139. 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.

140. 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.

141. Мальцев Г. Н., Вознюк В. В., Туктамышев М. Р. Моделирование конфликта сложных радиотехнических систем методом параллельных развивающихся стохастических процессов // Информационно-управляющие системы. 2013. № 5. С. 26-33.

142. Толстых Н.Н. Павлов В.А. Воробьева Е.И. Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем: учебное пособие. – Воронеж: ВГТУ, 2003. – 168 с.

143. Будников С. А. Модель обобщенного конфликта радиоэлектронных средств // Радиотехника. 2008. № 11. С. 8-10.

144. Будников С. А. Оценка вероятностных показателей в конфликте информационно-управляющих систем // Системы управления и информационные технологии. 2009. № 3(37). С. 27-31.

145. Бойко А. А. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84-92.

146. Бойко А. А. Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. № 5 (42). С. 196-211.

147. Мальцев Г. Н., Панкратов А. Н., Лесняк Д. А. Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1. С. 50-58.

148. Мальцев Г. Н., Теличко В. В. Оптимизация состава средств защиты в информационно-управляющей системе с каналами беспроводного доступа на основе графа реализации угроз // Информационно-управляющие системы. 2008. № 4. С. 29-33.

149. Бирюков Д. Н., Ломако А. Г. Метод синтеза сценариев упреждения на основе ассоциативно-рефлекторного поведения // Проблемы информационной безопасности. Компьютерные системы. 2015. № 1. С. 52-56.

150. Бирюков Д. Н., Ростовцев Ю. Г. Подход к построению непротиворечивой теории синтеза сценариев упреждающего поведения в конфликте // Труды СПИИРАН. 2015. № 1. С. 94-111.

151. 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.

152. Еремеев М. А., Ломако А. Г., Овчаров В. А., Акулов С. А., Коротков В. С., Свергун Н. В. Метод адаптивного управления активным сетевым оборудованием телекоммуникационной сети в условиях компьютерных атак // Информационное противодействие угрозам терроризма. 2012. № 19. С. 136-146.

153. Бирюков Д. Н., Ломако А. Г., Сабиров Т. Р. Многоуровневое моделирование сценариев упреждающего поведения // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 30-35.

154. Чукляев И. И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // T-Comm: Телекоммуникации и транспорт. – 2015. – №2. – С. 64-68.

155. Морозов А. В., Чукляев И. И. Информационная безопасность вычислительных систем боевого управления в аспекте информационного противоборства // Проблемы безопасности российского общества. 2013. № 2-3. С. 85-90.

156. Морозов А. В., Майбуров Д. Г., Чукляев И. И. Информационное оружие: теория и практика применения // Проблемы безопасности российского общества. 2014. № 2. С. 177-183.

157. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Военная мысль. 2012. № 7. С. 22-31.

158. Стародубцев Ю. И., Бухарин В. В., Семенов С. С. Техносферная война // Информационные системы и технологии. 2011. № 1. С. 80-85.

159. Стародубцев Ю. И., Семенов С. С., Бухарин В. В. Техносферная война // Научно-информационный журнал Армия и общество. 2010. № 4. С. 6-11.

160. 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.

161. Гриняев С. Н. Системы обнаружения вторжений и реагирования на компьютерные инциденты на основе мобильных программ-агентов. – М.: ЦСОиП, 2005. – 46 с.

162. Стародубцев Ю. И., Бухарин В. В., Кирьянов А. В., Баленко О. А. Метод оценки защищенности информационно-телекоммуникационной сети от деструктивных программных воздействий // Вестник компьютерных и информационных технологий. 2013. № 4 (106). С. 37-42.

163. Бухарин В. В., Кирьянов А. В., Стародубцев Ю. И. Способ защиты информационно-вычислительных сетей от компьютерных атак // Труды МАИ. 2012. № 57. С. 16.

164. Стародубцев Ю. И., Ерышов В. Г., Корсунский А. С. Модель

процесса мониторинга безопасности информации в информационно-телекоммуникационных системах // Автоматизация процессов управления. 2011. № 1. С. 58-61.

165. Шелухин О. И., Сакалема Д. Ж., Филинова А. С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / Под ред. О.И. Шелухина. – М.: Горячая линия-Телеком, 2013. – 220 с.

166. Коцыняк М. А., Кулешов И. А, Лаута О. С. Устойчивость информационно-телекоммуникационных сетей. – СПб.: Издательство Политехнического университета, 2013. – 93 с.

167. 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.

168. Остапенко Г. А., Колбасов С. М. Модели тактик реализации информационного конфликта // Информация и безопасность. 2006. Т. 9. № 1. С. 46-50.

169. Остапенко Г. А. Структурно-параметрическая модель информационного конфликта систем // Безопасность информационных технологий. 2007. № 2. С. 93-94.

170. Остапенко Г. А. Информационные операции и атаки в социотехнических системах. Монография. – Воронеж: Воронежский гос. технический ун-т, 2005. – 204 с.

171. Йоцов В. С., Сгурев В. С., Юсупов Р. М., Хомоненко А. Д. Онтологии для разрешения семантических конфликтов // Труды СПИИРАН. 2008. № 7. С. 26-40.

172. Емелин В. И. Методы и модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими системами. Дисс. … докт. техн. наук. – СПб: СПИИРАН, 2012. – 239 с.

173. Бухарин С. Н. Цыганов В. В. Методы и технологии информационных войн. – М.: Академический Проект, 2007. – 382 с.

174. Расторгуев С. П. Математические модели в информационном противоборстве. Экзистенциальная математика. – М.: АНО ЦСОиП, 2014. – 260 с.

175. Горбачев И. Е., Аниканов Г. А. Подход к снижению риска дезорганизации функционирования критической инфраструктуры в условиях информационного конфликта // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 106-119.

176. Поповский В. В., Лемешко А. В., Евсеева О. Ю. Динамическое управление ресурсами ТКС: математические модели в пространстве состояний // Наукові записки УНДІЗ. 2009. № 1 (9). С. 3-26.

177. Айзекс Р. Дифференциальные игры. – М.: Мир, 1967. – 480 с.

178. Понтрятин Л. С. К теории дифференциальных игр // Успехи математических наук. 1966. Т. 21. № 4. С. 219-274.

179. Красовский Н. Н., Субботин А. И. Позиционные дифференциальные игры. – М.: Наука, 1974. – 456 с.

180. Петросян Л. А Дифференциальные игры преследования. – Л.: ЛГУ, 1977. – 224с.

181. Николаев В. И., Толстых Н. Н. Адаптивное, ситуационное и рефлексивное управление подсистемой защиты информации автоматизированных телекоммуникационных комплексов // Теория и техника радиосвязи. 2006. № 2. С. 79-87.

182. Толстых Н. Н., Пятунин А. Н., Марейченко И. В., Павлов В. А., Слепов И. Ю. Принципы раннего обнаружения признаков конфликтного режима взаимодействия автоматизированных телекоммуникационных комплексов // Теория и техника радиосвязи. 2004. № 2. С. 115.

183. Смольяков Э.Р. Теория конфликтных равновесий. – М.: URSS, 2005.

184. Благодатских А. И., Петров Н. Н. Групповое преследование с фазовыми ограничениями в почти периодическом примере Л.С. Понтрягина // Дифференциальные уравнения. 2015. Т. 51. № 3. С. 387-394.

185. Юдицкий С. А. Техника графодинамического моделирования бинарных игр на основе сценарных связок // Управление большими системами. 2010. № 31. С. 289-298.

186. Юдицкий С. А. Графодинамическая автоматная модель разрешения конфликтов в организационных системах // Управление большими системами. 2008. № 23. С. 126-136.

187. Новиков Д. А. Сетевые структуры и организационные системы. – М.: ИПУ РАН, 2003. – 102 с.

188. Новиков Д. А. Механизмы функционирования многоуровневых организационных систем. – М.: Фонд "Проблемы управления", 1999. – 161 с.

189. Нгуен Куанг Тхыонг. Методы и модели надежности, эффективности и безопасности сложных технических систем в конфликтных ситуациях. Дис. ... д-ра техн. наук. – Тверь, 1999. – 322 с.

190. Таран Т. А. Логические методы и модели поддержки принятия решений в конфликтных ситуациях. Дис. … д-ра техн. наук. – М., 1998. – 266 с.

191. Борисов А. Н., Корнеева Г. В. Лингвистический подход к построению моделей принятия решений в условиях неопределенности // Методы принятия решений в условиях неопределенности: Сб. науч. тр. – Рига: Рижский политехнический институт. 1980. – С. 4-12.

192. Борисов А. Н., Алексеев А. В. Обработка нечеткой информации в системах принятия решений. – М.: Радио и связь, 1989. – 304 с.

193. Борисов А. Н., Крумберг О. А., Федоров И. П. Принятие решений на основе нечетких моделей: Примеры использования. – Рига: Зинатне, 1990. – 184 с.

194. Смирнов Ю.А. Радиотехническая разведка. – М.: Воениздат, 2001. – 456 с.

195. Алексеев А. А. Частотно-временной анализ сигналов связи и радиотехнического обеспечения. – Л.: ВАС, 1987. – 212 с.

196. Челышев В. Д., Якимовец В. В. Радиоэлектронные системы органов административного и военного управления. Ч. 1. – СПб.: ВАС, 2006. – 456 с.

197. Марчук Л. А. Пространственно-временная обработка сигналов в линиях радиосвязи. – Л.: ВАС, 1991. – 136 с.

198. Дворников С. В., Железняк В. К., Комарович В. Ф., Храмов Р. Н. Метод обнаружения радиосигналов на основе обработки их частотно-временных распределений плотности энергии // Информация и космос. 2005. № 4. С. 13-17.

199. Дворников С. В., Алексеева Т. Е. Распределение Алексеева и его применение в задачах частотно-временной обработки сигналов // Информация и космос. 2006. № 3 С. 9-21.

200. Захарченко А. Н., Веселов Ю. Г., Островский А. С., Сельвесюк Н. И., Метод оценки технического состояния цифровых оптико-электронных комплексов, адаптивный к условиям применения и решаемым задачам // Информатика и системы управления. 2015. № 5 (44). С. 33-44.

201. Кононов В. И. Теоретические основы радио- и радиотехнической разведки. – СПб: ВАС, 2000.

202. Замарин А. И., Атакищев О. И., Тавалинский Д. А., Рюмшин К. Ю. Последетекторный технический анализ цифровых последовательностей при идентификации сложных структур // Известия Юго-Западного государственного университета. 2014. № 1 (52). С. 14-21.

203. Замарин А. И., Тавалинский Д. А. Обобщенная модель построения процедур сокращения избыточности представления данных // Информация и космос. 2004. № 5. С. 52-74.

204. Саяпин В. Н., Дворников С. В., Симонов А. Н., Волков Р. В. Метод пространственно-временной фильтрации сигналов на основе антенных решеток произвольной пространственной конфигурации // Информация и космос. 2006. № 3. С. 83-89.

205. Комарович В. Ф., Саенко И. Б. Компьютерные информационные войны концепция и реалии // Защита информации. Конфидент. 2002. № 4-5. С. 84-88.

206. Ильин А. П., Шакин Н. К вопросу о месте радиоэлектронной разведки, радиоэлектронной борьбы и радиоэлектронной маскировки в информационной борьбе // Военная мысль. 2008. № 1. С. 25-30.

207. Мырова Л. О., Чепиженко А. З. Обеспечение стойкости аппаратуры связи к ионизирующим и электромагнитным излучениям. 2-е изд. – М.: Радио и связь, 1988. – 296 с.

208. Добыкин В. Д., Куприянов А. И., Пономарев В. Г., Шустов Л. Н. Радиоэлектронная борьба. Силовое поражение радиоэлектронных систем / Под ред. А.И. Куприянова. – М.: Вузовская книга, 2007. – 468 с.

209. Акбашев Б. Б., Балюк Н. В., Кечиев Л. Н. Защита объектов телекоммуникаций от электромагнитных воздействий. – М.: Грифон, 2014. – 472 с.

210. Гизатуллин Р. М., Гизатуллин З. М. Помехоустойчивость и

информационная безопасность вычислительной техники при электромагнитных воздействиях по сети электропитания. Монография. – Казань: Изд-во Казан. гос. техн. ун-та, 2014. – 142 с.

211. Михайлов В. А. Разработка методов и моделей анализа и оценки устойчивого функционирования бортовых цифровых вычислительных комплексов в условиях преднамеренного воздействия сверхкоротких электромагнитных излучений. Дисс. … докт. техн. наук. – М.: НИИ «Аргон», 2014. – 390 с.

212. Михеев О. В. Средства измерений и методы испытаний телекоммуникационных систем в условиях воздействия электромагнитных импульсов с субнаносекундной длительностью фронта. Дисс. … канд. техн. наук. – М.: МИЭМ НИУ ВШЭ, 2006. – 162 с.

213. Хохлов Н. С., Сидоров А. В. Оценка устойчивости системы радиосвязи и управления к деструктивным электромагнитным воздействиям // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. 2013. № 2 (18). С. 27-35.

214. Сидоров А. В. Оценка устойчивости средств радиосвязи и управления органов внутренних дел к деструктивным электромагнитным воздействиям. Дисс. … канд. техн. наук. – Воронеж: ВИ МВД России, 2015. – 149 с.

215. Якушин С. П. Методы и средства оценки воздействия электромагнитного импульса большой энергии на телекоммуникационные сети. Дисс. … канд. техн. наук. – М.: МИЭМ НИУ ВШЭ, 2004. – 146 с.

216. Климов С. М. Методы и модели противодействия компьютерным атакам. – Люберцы.: Каталист, 2008. – 316 с.

217. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Методические основы: Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. – 108 с.

218. Белоножкин В. И., Остапенко Г. А. Информационные аспекты противодействия терроризму. – М.: Горячая линия - Телеком, 2009. – 112 с.

219. Дёшина А.Е., Бурса М. В., Остапенко А. Г., Калашников А. О., Остапенко Г. А. Управление информационными рисками мультисерверных систем при воздействии DDOS-атак / Под ред. Д.А. Новикова. Воронеж: Научная книга, 2014. 160 с.

220. Бутузов В. В., Бурса М. В., Остапенко А. Г., Калашников А. О., Остапенко Г.А. Информационные риски флуд-атакуемых компьютерных систем / Под ред. Д.А. Новикова. – Воронеж: Научная книга, 2015. – 160 с.

221. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – М.: Радио Софт, 2011. – 229 с.

222. Язов Ю.К., Сердечный А.Л., Бабурин А.В. Метод формализации процесса несанкционированного доступа в информационных системах, построенных с использованием средств виртуализации, основанный на

математическом аппарате сетей Петри // Информация и безопасность. 2013. Т. 16. № 4. С. 518-521.

223. Аграновский А. В., Репалов С. А., Хади Р. А., Якубец М. Б. О недостатках современных систем обнаружения вторжений // Телекоммуникации. 2005. № 1. С. 39.

224. Аграновский А. В., Хади Р. А. Новый подход к защите информации - системы обнаружения компьютерных угроз // Информационный бюллетень РФФИ. 2007. № 4. С. 22.

225. Аграновский А. В., Хади Р. А., Якубец М. Б. Статистические методы обнаружения аномального поведения в системах обнаружения атак // Информационные технологии. 2005. № 1. С. 18.

226. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие. – М: Горячая линия-Телеком, 2004. – 280 с.

227. Исупов А. Б. Моделирование процесса функционирования телекоммуникационной сети в условиях программно-аппаратных воздействий // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2012. № 81. С. 103-114.

228. Исупов А. Б. Многоуровневый бионический алгоритм для обнаружения и идентификации программно-аппаратных воздействий на информационно-телекоммуникационные сети // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2012. № 81. С. 76-92.

229. Привалов А. А., Попов П. В. Электромагнитная совместимость средств связи и её влияние на устойчивость функционирования системы связи ВМФ в условиях воздействия противника оружием функционального поражения // Технологии электромагнитной совместимости. 2004. № 4. С. 65-68.

230. Привалов А. А., Попов П. В. Электромагнитная совместимость средств связи и её влияние на устойчивость функционирования системы связи ВМФ в условиях воздействия противника оружием функционального поражения // Технологии электромагнитной совместимости. 2004. № 11. С. 65-67.

231. Ададуров С. Е., Елишев В. В., Ефимов В. П. Проблемы передачи информации в многоспутниковых сетевых системах. – М.: МО РФ, 1996. – 120 с.

232. Ададуров С. Е., Астанин А.В., Мальцев Г.Н., Рязанов С.Н., Степанов М.Г. и др. Моделирование сетевых спутниковых систем передачи информации. – М.: МО РФ, 1996. – 125 с.

233. Перегудов М. А., Бойко А. А. Модель процедуры случайного множественного доступа к среде типа S-Aloha // Информационно-управляющие системы. 2014. № 6. С. 75-81.

234. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

235. Прилепский В. В. Конфликты в информационно-телекоммуникационных системах: учебное пособие. Часть 1. – Воронеж: ВГУ. 2004. – 145 с.

236. Левин В.И. Логико-алгебраический подход к моделированию конфликтов // Системы управления, связи и безопасности. 2015. № 4. С. 69-87.

237. Левин В. И. Автоматное моделирование исторических процессов на примере войн // Радиоэлектроника. Информатика. Управление. 2002. № 12. С. 93-101.

238. Левин В. И. Автоматное моделирование процессов возникновения и распада коллектива // Кибернетика и системный анализ. 2003. № 3. С. 92–101.

239. Мистров Л. Е. Конфликтная устойчивость взаимодействия организационно-технических систем: общие понятия, научные подходы, метод синтеза // Наукоемкие технологии. 2011. Т. 12. № 9. С. 70-80.

240 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.

241. 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.

242. Козирацкий Ю. Л., Кущев 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.

243. Тарасов А. А. Функциональная отказоустойчивость систем обработки информации. Монография. – М.: МИНИТ ФСБ России, 2009. – 181 с.

244. Жуматий В. П., Будников С. А., Паршин Н. В. Угрозы программно-математического воздействия. – Воронеж: ЦПКС ТЗИ, 2010. – 230 с.

245. 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.

246. 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.

247. Бойко А. А., Храмов В. Ю. Модель информационного конфликта информационно-технических и специальных программных средств в вооруженном противоборстве группировок со статичными характеристиками // Радиотехника. 2013. № 7. С. 5-10.

248. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С. 57-68.

249. 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.

250. 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.

251. 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.

252. Алферов А. Г., Толстых И. О., Толстых Н. Н., Поздышева О. В., Мордовин А. И. Усточивость инфокоммуникационных систем в условиях информационного конфликта // Информация и безопасность. 2014. Т. 17. № 4. С. 558-567.

253. Стюгин М. А. Постановка задачи дезинформации в информационных системах // Информационные войны. 2014. № 3 (31). С. 6-11.

254. Стюгин М. А. Методика достижения информационного превосходства в конфликтных системах // Информационные войны. 2013. № 3 (27). С. 17-21.

255. Стюгин М. А. Рефлексивно-сигнатурный анализ конфликта // Искусственный интеллект и принятие решений. 2012. № 2. С. 39-50.

256. Стюгин М. А. Планирование действий в конфликте на уровне функциональных структур // Информационные войны. 2009. № 2. С. 16-21.

257. Шевцов В. А. Информационное противоборство как крайнее проявление конфликта в информационном пространстве // Радиотехника. 2001. № 3. С. 87-93.

258. Новиков С. Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / Под редакцией В.П. Шувалова. – М.: Горячая линия - Телеком, 2015. – 128 с.

259. Якушенко С. А., Прасько Г. А., Дворовой М. О., Веркин С. С. К вопросу решения антагонистических задач при комплексном противодействии сторон // Наукоёмкие технологии в космических исследованиях Земли. 2012. № 1. С. 24-26.

260. 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.

261. Григорьев В. Р., Шуркин Л. О. Сетецентрические войны с позиции синергетики // Вестник Российского государственного гуманитарного университета. 2014. № 11. С. 67-100.

262. Паршуткин А. В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем //

Вопросы кибербезопасности. 2014. № 5 (8). С. 2-6.

263. 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.

264. Исаев В. В., Бабусенко С. И. Статистическое моделирование многопролетных сетей пакетной радиосвязи // Техника средств связи: материалы 18 научно-технической конференции. – Воронеж: НИИС, 1992.

265. Бабусенко С. И., Исаев В. В. Аналитическая модель маршрутизации в пакетной сети // Техника средств связи: материалы 18 научно-технической конференции. – Воронеж: НИИС, 1992.

266. Бабусенко С. И. Модель процесса радиоподавления пакетной радиосети с протоколом ненастойчивого доступа с прослушиванием несущей // Тезисы докладов 31 ВНТК академии. – Л.: ВАС, 1990.

267. Зима В. М., Котухов М. М., Ломако А. Г., Марков А. С., Молдовян А.А. Разработка систем информационно-компьютерной безопасности. – СПб.: ВКА, 2003. – 327 с.

268. Алферов А. Г., Мордвин А. И., Толстых Н. Н., Поздышева О. В. Эффектность систем управления связью при ограничении ресурса в режиме информационного конфликта // Информация и безопасность. 2014. Т. 17. № 4. С. 548-557.

269. Царегородцев А. В. Методы, модели и алгоритмы синтеза защищенных информационных систем. – М.: ВГНА Минфина России, 2009. – 207 с.

270. Царегородцев А. В. Организация защиты объектов информатизации от силовых деструктивных электромагнитных воздействий // Национальная безопасность / nota bene. 2011. № 3. С. 139-152.

271. Царегородцев А. В. Рекомендации по защите объектов информатизации от деструктивных электромагнитных воздействий // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2012. № 4-5. С. 38-48.

272. Воскобович В. В., Михайлов В. А., Мырова Л. О., Царегородцев А. В. Системный подход к созданию методологии анализа и оценки устойчивости ИКС к деструктивному воздействию ЭМИ // Технологии электромагнитной совместимости. 2012. № 1. С. 51-58.

273. Макаренко С. И. Оценка качества обслуживания пакетной радиосети в нестационарном режиме в условиях воздействия внешних дестабилизирующих факторов // Журнал радиоэлектроники. 2012. № 6. С. 2. – URL: http://jre.cplire.ru/jre/jun12/9/text.pdf (дата доступа 26.08.2016).

274. Макаренко С.И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2. – URL: http://jre.cplire.ru/jre/sep11/4/text.pdf (дата доступа 26.08.2016).

275. Гречишников Е. В., Горелик С. П., Добрышин М. М. Способ обеспечения требуемой защищённости сети связи от внешних деструктивных воздействий // Телекоммуникации. 2015. № 6. С. 30-37.

276. Гречишников Е. В., Белов А. С., Шумилин В. С. Способ управления защищенностью сетей связи в условиях деструктивных программных воздействий // Телекоммуникации. 2014. № 3. С. 18-22.

277. Гречишников Е. В., Горелик С. П., Белов А. С. Предложения по обеспечению живучести элементов сетей связи в чрезвычайных ситуациях // Телекоммуникации 2013. № 4. С. 23-26.

278. Гречишников Е. В., Гусев А. П. Обеспечение устойчивости системы связи в условиях сверхвысокочастотного электромагнитного излучения // Телекоммуникации. 2011. № 10. С. 37-41.

279. Котенко Д. И., Котенко И. В., Саенко И. Б. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. № 3 (22). С. 5-30.

280. Котенко И. В., Саенко И. Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. № 3 (22). С. 84-100.

281. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 1 (24). С. 21-40.

282. Зегжда Д. П., Коваленко С. Л. Проблемы безопасности беспроводных сетей семейства IEEE 802.11a/b/g // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 45-49.

283. Зегжда Д. П., Коротич А. В. Контроль доступа к информационным ресурсам в информационно-телекоммуникационных системах высокой доступности // Наукоемкие технологии. 2007. Т. 8. № 11. С. 41-46.

284. Зегжда П. Д. Основные направления развития технологии обеспечения безопасности в эпоху информационного противоборства // Проблемы информационной безопасности. Компьютерные системы. 2007. № 1. С. 60-72.

285. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. – Череповец: ЧВВИУРЭ, 2016. – 128 с.

286. Вавилов В. А., Назаров А. А. Исследование устойчивых сетей множественного доступа с источником повторных вызовов, функционирующим в случайной среде // Вычислительные технологии. 2008. Т. 13. № 5. С. 14-18.

287. Вишневский В. М., Ляхов А. И. Оценка производительности беспроводной сети в условиях помех // Автоматика и телемеханика. 2000. № 12. С. 87-103.

288. Елесин М. Е., Ходаревский Д. Н. Аналитическая модель влияния вероятности ошибки в радиоканале на характеристики пакетной передачи сети беспроводного доступа // Актуальные проблемы развития технологических систем государственной охраны, специальной связи и специального информационного обеспечения: VIII Всероссийская межведомственная научная

конференция: материалы и доклады (Орёл, 13–14 февраля 2013 г.). – Орёл: Академия ФСО России, 2013. С. 36-40.

289. Ковальков Д. А. Динамический анализ радиоканала случайного доступа системы связи с расширением спектра и ретрансляцией сигналов // Инфокоммуникационные технологии. 2009. Т. 7. № 1. С. 23-29.

290. Осипов Д. С. Система множественного доступа, использующая некогерентный пороговый прием, частотно-позиционное кодирование и динамически выделяемый диапазон частот, в условиях подавления полезного сигнала // Информационно-управляющие системы. 2010. № 6. С. 28-32.

291. Спирина Е. А. Оптимизация распределения информации в фиксированных сетях широкополосного радиодоступа с учётом внутрисистемных помех // Журнал радиоэлектроники. 2015. № 9. – URL: http://jre.cplire.ru/jre/sep15/5/text.pdf (дата доступа 26.08.2016).

292. Чакрян В. Р. Многомерные стохастические и имитационные модели телетрафика и каналов передачи данных в условиях помех. Дис. … канд. техн. наук: 05.13.18 / Чакрян Вячеслав Робертович – Ростов-на-Дону, 2009. – 157 с.

293. Поповский В. В., Волотка В. С. Методы анализа динамических структур телекоммуникационных систем // Восточно-Европейский журнал передовых технологий. 2013. № 5/2 (65). С. 18-22.

294. Поповский В. В., Волотка В. С. Математическое моделирование надежности инфокоммуникационных систем // Телекомунікаційні та інформаційні технології. 2014. № 3. С. 5-9.

295. Поповский В. В., Лемешко А. В., Мельникова Л. И., Андрушко Д. В. Обзор и сравнительный анализ основных моделей и алгоритмов многопутевой маршрутизации в мультисервисных телекоммуникационных сетях // Прикладная радиоэлектроника. 2005. Т. 4. № 4. С. 372-382. – URL: http://alem.ucoz.ua/_ld/0/10_Lemeshko_PRE_20.pdf (дата доступа 01.05.2015).

296. Лемешко А. В., Евсеева О. Ю., Дробот О. А. Методика выбора независимых путей с определением их количества при решении задач многопутевой маршрутизации // Праці УНДІРТ. 2006. № 4 (48). С. 69-73. – URL: http://alem.ucoz.ua/_ld/0/14_Lemeshko_UNIIRT.pdf (дата доступа 01.05.2015).

297. Лемешко А. В., Козлова Е. В., Романюк А. А. Математическая модель отказоустойчивой маршрутизации, представленная алгебраическим уравнениями состояния MPLS-сети // Системи обробки інформації. 2013. № 2 (109). С. 217-220.

298. Попков В. К. Математические модели связности. Новосибирск: Изд. ИВМиМГ СО РАН, 2006. 490 с.

299. Попков В. К., Блукке В. П., Дворкин А. Б. Модели анализа устойчивости и живучести информационных сетей // Проблемы информатики. 2009. № 4. С. 63-78.

300. Сорокин А. А., Дмитриев В. Н. Описание систем связи с динамической топологией сети при помощи модели «мерцающего» графа // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика.

2009. № 2. С. 134-139.

301. Сорокин А. А., Дмитриев В. Н., Чан Куок Тоан, Резников П. С. Оценка результатов использования протокола RIP в системах связи с динамической топологией сети методом имитационного моделирования // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2014. № 4. С. 85-93.

302. Перепелкин Д. А. Алгоритм парных перестановок маршрутов на базе протокола OSPF при динамическом отказе узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2014. № 1 (47). С. 84-91.

303. Перепелкин Д. А. Алгоритм адаптивной ускоренной маршрутизации? на базе протокола IGRP при динамическом отказе узлов и линий связи корпоративной сети // Вестник Рязанского государственного радиотехнического университета. 2012. № 4 (42). С. 33-38.

304. Перепелкин Д. А. Динамическое формирование структуры и параметров линий связи корпоративной сети на основе данных о парных перестановках маршрутов // Информационные технологии. 2014. № 4. С. 52-60.

305. Корячко В. П., Перепелкин Д. А. Анализ и проектирование маршрутов передачи данных в корпоративных сетях. М.: Горячая линия – Телеком, 2012. 236 с.

306. Мейкшан В. И. Анализ влияния отказов оборудования на функционирование мультисервисной сети с адаптивной маршрутизацией // Доклады академии наук высшей школы Российской Федерации. Технические науки. 2010. № 2 (15). С. 69-80.

307. Горев П. Г., Назаров А. С., Пасечников И. И. Определение связности в путевом пространстве состояний телекоммуникационной сети // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2012. Т. 17. № 5. С. 1360-1363.

308. Литвинов К. А., Пасечников И. И. Подходы к решению задачи маршрутизации в современных телекоммуникационных системах // Вестник Тамбовского университета. Серия: Естественные и технические науки. 2013. Т. 18. № 1. С. 64-69.

309. Громов Ю. Ю., Драчев В. О., Набатов К. А., Иванова О. Г. Синтез и анализ живучести сетевых систем: монография. – М.: «Издательство Машиностроение-1», 2007. – 152 с.

310. Ковальков Д. А. Математические модели оценки надежности мультисервисного узла доступа // Радиотехнические и телекоммуникационные системы. 2011. № 2. С. 64-71.

311. Горбунов И. Э. Методология анализа и синтеза реконфигурируемых топологий мобильной связи // Математичні машини і системи. 2006. № 2. С. 48-59.

312. Егунов М. М., Шувалов В. П. Анализ структурной надёжности транспортной сети // Вестник СибГУТИ. 2012. № 1. С. 54-60.

313. Ластовченко М. М., Зубарева Е. А., Саченко В. О. Метод анализа

эффективности реконфигурации топологии построения беспроводных мультисервисных сетей повышенной помехозащищенности // Управляющие системы и машины. 2009. № 6. С. 79-86.

314. Стромов А. В., Нечаев Ю. Б., Баев А. Д. Моделирование маршрутизации в беспроводной ячеистой сети с адаптацией к воздействию нескольких источников помех // Теория и техника радиосвязи. 2014. № 4. С. 46-52.

315. Цимбал В. А., Тоискин В. Е., Якимова И. А., Косарева Л. Н. Нахождение границ применимости протокола TCP в сетях связи с низкоскоростными каналами // XXIII Всероссийская научно-техническая конференция. – Серпухов: ВА РВСН (филиал г. Серпухов), 2014. – С. 290-259.

316. Тоискин В. Е., Цимбал В. А., Якимова И. А., Кабанович С.Г . Марковская модель доведения многопакетных сообщений по стеку протоколов TCP/IP с процедурой «скользящее окно» // Международная конференция RES-2014. – М.: Российское научно-техническое общество радиотехники, электроники и связи имени А.С. Попова, 2014. – С. 112-114.

317. Свинцов А. А., Солодуха Р. А. Аналитическая модель функционирования линии передачи данных с решающей обратной связью и оконным управлением потоком в условиях воздействия помех // Вестник Воронежского института МВД России. 2007. № 2. С. 197-202.

318. 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.

319. 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 01.08.2016).

320. Макаренко С. И. Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности. 2015. № 2. С. 45-98. – URL: http://sccs.intelgr.com/archive/2015-02/03-Makarenko.pdf (дата обращения 01.08.2016).

321. Макаренко С. И., Михайлов Р. Л. Модель функционирования маршрутизатора в сети в условиях ограниченной надежности каналов связи // Инфокоммуникационные технологии. 2014. Т. 12. № 2. С. 44-49.

322. 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.

323. 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://sccs.intelgr.com/archive/2015-01/07-Makarenko.pdf (дата обращения

01.08.2016).

324. Власов Ю. Б., Николаев В. И., Толстых И. О., Толстых Н. Н., Челядинов Ю. В. Оценка потенциальной опасности потоков данных в инфокоммуникационной системе // Радиотехника. 2012. № 8. С. 33-40.

325. Макаренко С. И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. // Вопросы кибербезопасности. № 3 (4). 2014. С. 7-13.

326. Ушанев К. В. Имитационные модели системы массового обслуживания типа *Pa*/*M*/1, H_2/*M*/1 и исследование на их основе качества обслуживания трафика со сложной структурой // Системы управления, связи и безопасности. 2015. № 4. С. 217-251. URL: http://journals.intelgr.com/sccs/archive/2015-04/14-Ushanev.pdf (дата обращения 26.08.2016).

327. 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.

328. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.

329. Гуревич И. М. Многоуровневая модель сети связи // Вопросы кибернетики. Протоколы и методы коммутации в вычислительных сетях. 1986. С. 72-88.

330. 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.

331. Гуревич И. М. Динамическая модель сети связи // Теория телетрафика в системах информатики. 1989. С. 77-86.

332. Гуревич И. М. Динамические свойства сетевых систем // Вопросы кибернетики. Архитектура и протоколы вычислительных сетей. 1990. С. 22-44.

333. Вакуленко А. А., Шевчук В. И. Математическая модель динамики конфликта радиоэлектронных систем // Радиотехника. 2011. № 1. С. 56-59.

334. Маевский Ю. И. Основные положения методологии синтеза многофункциональной конфликтно-устойчивой системы радиоэлектронной борьбы // Радиотехника. 2010. № 6. С. 61-66.

335. 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.

336. Семенова И. И., Мишурин А. О. Система управления моделями в области информационного противоборства // Вестник Саратовского государственного технического университета. 2010. Т. 4. № 1 (49). С. 150-160.

337. Веселов Г. Е., Колесников А. А. Синергетический подход к

обеспечению комплексной безопасности сложных систем // Известия ЮФУ. Технические науки. 2012. № 4 (129). С. 8-18.

338. Яковлев В. Б., Колесников А. А. Синергетическое управление нелинейными объектами с хаотической динамикой // Известия ЮФУ. Технические науки. 2001. № 5 (23). С. 126-131.

339. Базыкин А. Д. Нелинейная динамика взаимодействующих популяций. – Москва-Ижевск: Институт компьютерных исследований, 2003. – 368 с.

340. Котенко И. В., Уланов А. В. Команды агентов в киберпространстве: моделирование процессов защиты информации в глобальном Интернете // Труды Института системного анализа Российской академии наук. 2006. Т. 27. С. 108-129.

341. Котенко И. В., Уланов А. В. Компьютерные войны в интернете: моделирование противоборства программных агентов // Защита информации. Инсайд. 2007. № 4 (16). С. 38-45.

342. Котенко И. В., Уланов А. В. Многоагентное моделирование защиты информационных ресурсов в сети Интернет // Известия Российской академии наук. Теория и системы управления. 2007. № 5. С. 74-88.

343. Вайпан С. Н., Вакуленко А. А., Верба В. С., Ягольников С. В. Показатели оценки конфликтной устойчивости функционирования РЭС в условиях информационного противоборства // Радиотехника. 2006. № 1. С. 46-49.

344. Вакуленко А. А., Шевчук В. И., Ягольников С. В. Оценка эффективности радиоэлектронной системы в динамике конфликта // Радиотехника. 2009. № 9. С. 84-86.

345. Власов В. В., Шевчук В. И., Шевчук Д. В., Ягольников С. В. Метод синтеза космической системы дистанционного зондирования земли в условиях сложного информационного конфликта // Радиотехника. 2015. № 3. С. 57-63.

346. Вакуленко А. А., Верба В.С., Дод В. Н. Организация конфликтно-устойчивого управления интегрированной радиоэлектронной системой в динамике конфликта со средствами радиоэлектронного подавления // Радиотехника. 2006. № 1. С. 50-53.

347. Николаев В. И., Толстых Н. Н., Алферов А. Г., Степанец Ю. А., Толстых И. О., Ролдугин Н. Г., Артемов М. В. Принудительный синтез заданного целевого состояния процессорного устройства: концепция перехвата управления // Радиотехника. 2016. № 5. С. 84-96.

348. Верба В. С., Дёмин А. Н., Хрипунов С. П. Принципы построения системы прогнозирования развития конфликтных ситуаций // Радиотехника. 2010. № 8. С. 20-25.

349. Меркулов В. И., Добыкин В. Д., Дрогалин В. В. Функциональное поражение радиоэлектронных систем // Фазотрон. 2006. № 3. С. 4.

350. Дрогалин В. В., Казаков В. Д., Меркулов В. И. Преднамеренные алгоритмические воздействия на цифровые вычислительные системы авиационных радиолокационных систем // Фазотрон. 2007. № 1. С. 2.

351. Меркулов В. И., Забелин И. В. Траекторное управление наблюдением как способ создания преднамеренных алгоритмических воздействий на радиолокационные системы // Радиотехника. 2010. № 7. С. 77-81.

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

353. Евглевская Н. В., Привалов А. А., Привалов А. А. Обобщенная модель информационного воздействия на автоматизированные системы управления техническими объектами // Вопросы радиоэлектроники. 2013. Т. 3. № 1. С. 155-164.

354. Евглевская Н. В., Привалов А. А., Привалов А. А. Модель процесса вскрытия каналов утечки информации на объектах телекоммуникаций // Вопросы радиоэлектроники. 2014. Т. 3. № 1. С. 156-161.

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

356. Евглевская Н. В., Привалов А. А. Модель информационного воздействия на объекты телекоммуникационной сети // Известия Петербургского университета путей сообщения. 2015. № 1 (42). С. 72-77.

357. Привалов А. А., Привалов А. А., Скуднева Е. В., Чалов И. В. Подход к оценке вероятности вскрытия пространственно-временной и информационной структуры СПД-ОТН // Известия Петербургского университета путей сообщения. 2015. № 3 (44). С. 165-172.

358. Левин В. И., Немкова Е. А. Логико-математическое моделирование конфликтов // Системы управления, связи и безопасности. 2016. № 3. С. 55-64. URL: http://sccs.intelgr.com/archive/2016-03/02-Levin.pdf (дата обращения 20.08.2016).

359. Йоцов В. С. Разрешение семантических конфликтов с использованием онтологий // Proc. 2nd Intl. Conference on System Analysis and Information Technologies, SAIT. 2007. С. 11-14. – URL: http://195.96.242.2/staff_en/V_Jotsov/p68Caluga07.pdf (дата обращения 20.08.2016).

360. Когаловский М. Р. Методы интеграции данных в информационных системах. – М.: Институт проблем рынка РАН, 2010. С. 1-9. – URL: http://www.ipr-ras.ru/articles/kogalov10-05.pdf (дата обращения 20.08.2016).

361. Брюхов Д. О., Вовченко А. Е., Захаров В. Н., Желенкова О. П., Калиниченко Л. А., Мартынов Д. О., Скворцов Н. А., Ступников С. А. Архитектура промежуточного слоя предметных посредников для решения задач над множеством интегрируемых неоднородных распределенных информационных ресурсов в гибридной грид-инфраструктуре виртуальных обсерваторий // Информатика и ее применение. 2008. Том 2. № 1. С. 2-34.

362. Андреев А. М., Березкин Д. В., Кантонистов Ю. А. Выбор СУБД для построения информационных систем корпоративного уровня на основе объектной парадигмы // СУБД. 1998. № 4-5. С. 26-50. – URL: http://www.inteltec.ru/publish/articles/objtech/4kx4_9.shtml (дата обращения: 25.08.2016).

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

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

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

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

367. Воробьев Н. Н. Основы теории игр. Бескоалиционные игры. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 496 с.

368. Чуднов А. М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации. 1991. Том 27. № 3. С. 57-65.

369. Жодзишский М. И. Применение теории игр к синтезу оптимальной системы посимвольной передачи информации // Радиотехника. 1982. № 11. С. 77-81.

370. Bazar T., Wu Y. A Complete Characterization of Minimax and Maximin Encode-Decoder Policies for Communication Channels with Incomplete Statistical Description // IEEE Transactions on Information Theory. 1985. Vol. 31. № 4. Pp. 482-489.

371. Cahn C. Performance of Digital Matched Filter Correlator with Unknown Interference // IEEE Transactions on Information Theory. 1971. Vol. 19. № 6. Pp. 1163-1172.

372. Блекуэлл Д., Гиршик М. А. Теория игр и статистических решений / Пер с англ. под ред. Б.А. Севостьянова. – М.: Иностранная литература, 1958. – 374 с.

373. Данскин Дж. М. Теория максимина. – М.: Сов. радио, 1970. – 200 с.

374. Нейман Д., Моргенштерн О. Теория игр и экономическое поведение. – М.: Наука, 1970. – 707 с.

375. Партхасаратхи Т., Рагхаван Т. Некоторые вопросы теории игр двух лиц. – М.: Мир, 1974. – 295 с.

376. Петросян Л. А., Томский Г. В. Динамические игры и их приложения. – Л.: ЛГУ, 1982. – 252 с.

377. Черноусько Ф. Л., Меликян А. А. Игровые задачи управления и поиска. – М.: Наука, 1978. – 270 с.

378. Козлов Д. Г. Реальная гарантированная помехоустойчивость асимптотически оптимального игрового приемника псевдошумового сигнала //

Техника средств связи. 1988. № 2. С. 42-52.

379. Путилин А. Н. Радиосистемы с множественным доступом. – СПб.: ВАС, 1998. – 148 с.

380. Путилин А. Н. Модель взаимодействия линии радиосвязи и станции радиоэлектронного подавления // Труды XIII Санкт-Петербургской международной конференции «Региональная информатика (РИ-2012)». – СПб.: СПОИСУ, 2013. С. 196-207.

381. Путилин А. Н. Модель функционирования сети радиосвязи в условиях радиоэлектронного подавления // Сборник тезисов докладов научной конференции «Современные тенденции развития теории и практики управления в системах специального назначения». – М.: «Концерн «Системпром», 2013. С. 102.

382. Юдицкий С. А. Моделирование динамики многоагентных триадных сетей. – М.: СИНТЕГ, 2012. – 112 с.

References

1. Budnikov S. A., Grevtsev A. I., Ivantsov A. V., Kil'diushevskii 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. Monograph]. Moscow, Radiotekhnika Publ., 2013. 232 p. (in Russian).

2. Gavrilov V. M. *Optimal'nye protsessy v konfliktnykh situatsiiakh* [Optimal processes in conflict situations]. Moscow, Sov. Radio Publ., 1969. 160 p. (in Russian).

3. Krapivin V. F. *Teoretiko-igrovye metody sinteza slozhnykh sistem v konfliktnykh situatsiiakh* [Game-theoretic methods for the synthesis of complex systems in conflict situations]. Moscow, Sov. Radio Publ., 1972. 192 p. (in Russian).

4. Lefevr V. A. *Konfliktuiushchie struktury* [Conflicting structures]. Moscow, Sov. Radio Publ., 1973. 159 p. (in Russian).

5. Saaty T. L. *Mathematical models of arms control and disarmament: application of mathematical structures in politics*. Vol. 14. – John Wiley & Sons, 1968.

6. Mesarovic M. D., Macko D., Takahara Y. *Theory of multilevel hierarchical systems*. New York, Academic. 1970.

7. Mesarovic M. D. Takahara Y. *General systems theory: mathematical foundationsm*. New York, Academic press, 1975.

8. Danilov N. N. *Igrovye modeli priniatiia reshenii* [Game models of decision-making]. Kemerovo, 1981. 122 p. (in Russian).

9. Berzin E. L. *Optimal'noe raspredelenie resursov i teoriia igr* [Optimal resource allocation and game theory]. Moscow, Radio i Sviaz Publ., 1983. 216 p. (in Russian).

10. Kukushkin N. S., Menshikova O. R., Menshikov I. S. *Konflikty i kompromissy* [Conflicts and trade-offs]. Moscow, Znanie Publ., 1986. 32 p. (in Russian).

11. Gorelik V. A., Kononenko A. F. *Teoretiko-igrovye modeli priniatiia reshenii v ekologo-ekonomicheskikh sistemakh* [Game-theoretic models of decision-making in ecological and economic systems]. Moscow, Radio i Sviaz Publ., 1982. 144 p. (in Russian).

12. Gorelik V. A., Gorelov M. A., Kononenko A. F. *Analiz konfliktnykh situatsii v sistemakh upravleniia* [The analysis of conflict situations in control systems]. Moscow, Radio i Sviaz Publ., 1991. 288 p. (in Russian).

13. Chikrii A. A. *Konfliktno-upravliaemye protsessy* [Conflict-controlled processes]. Kiev, Naukova Dumka Publ., 1992. 383 p. (in Russian).

14. Burkov V. N., Danaev B., Enaliev A. K., Kondratev V. V., Naneva T. B., Shepkin A. V. *Bol'shie sistemy: modelirovanie organizatsionnykh mekhanizmov* [Big systems: modelling of organizational mechanisms]. Moscow, Nauka Publ., 1989. 246 p. (in Russian).

15. Burkov V. N., Irikov V. A. *Modeli i metody upravleniia organizatsionnymi sistemami* [Models and management methods organizational systems]. Moscow, Nauka Publ., 1994. 270 p. (in Russian).

16. Malafeev O. A., Muravev A. I. *Matematicheskie modeli konfliktnykh situatsii i ikh razreshenie. Tom 1. Obshchaia teoriia i vspomogatel'nye svedeniia* [A mathematical model of conflict situations and their resolution. Vol. 1. General theory and supporting data]. Saint-Petersburg, Saint-Petersburg State University of Economics, 2000. 283 p. (in Russian).

17. Svetlov V. A. *Analitika konflikta* [Analyst conflict]. Saint-Petersburg, Rostok Publ., 2001. 511 p. (in Russian).

18. Novoseltsev V. I. *Sistemnaia konfliktologiia* [System conflict]. Voronezh, Kvarta Publ., 2001. 169 p. (in Russian).

19. Novikov D. A., Chkhartishvili A. G. *Refleksivnye igry* [Reflexive games]. Moscow, SINTEG Publ., 2003. 149 p. (in Russian).

20. 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).

21. Novikov D. A. *Teoriia upravleniia organizatsionnymi sistemami* [Theory of control of organizational systems], 2-th edition. Moscow, Fizmatlit Publ., 2007. 584 p. (in Russian).

22. 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, Izdatelsvo fiziko-matematicheskoi literatury, 2010. 228 p. (in Russian).

23. Mistrov L. E., Serbulov Ju. S. *Metodologicheskie osnovy sinteza informatsionno-obespechivaiushchikh funktsional'nykh organizatsionno-tekhnicheskikh sistem* [Methodological bases of synthesis of information-providing functional organizational-engineering systems]. Voronezh, Nauchnaia Kniga Publ., 2007. 232 p. (in Russian).

24. Mistrov L. E. *Modelirovanie informatsionnykh struktur obespecheniia konfliktnoi ustoichivosti vzaimodeistviia organizatsionno-tekhnicheskikh sistem.* Diss.

Doc. Eng. nauk [Modeling the information structures of the conflict ensure the stability of the interaction of organizational-technical systems. Dr. habil. Tesis]. Tambov, 2008. 435 p. (in Russian).

25. Serbulov Ju. S. *Modeli vybora i raspredeleniia resursov tekhnologicheskikh sistem v usloviiakh ikh zameshcheniia i konflikta*. Diss. Doc. Eng. nauk [Model selection and resource allocation of technological systems in terms of their substitution and conflict]. Voronezh, 1999. 306 p. (in Russian).

26. Velichko S. V., Mistrov L. E., Serbulov Ju. S. *Metodologicheskie osnovy sinteza reshenii po upravleniiu ekologicheskimi konfliktami* [Methodological bases of synthesis of solutions for managing environmental conflicts]. Voronezh, Nauchnaia Kniga Publ., 2008. 386 p. (in Russian).

27. Ougolnitsky G. A. *Ierarkhicheskoe upravlenie ustoichivym razvitiem* [Hierarchical control of sustainable development]. Moscow, Fiziko-Matematicheskoi Literatury Publ., 2010. 336 p. (in Russian).

28. Ougolnitsky G. A., Usov A. B. The sustainable development of the management systems in the conditions of corruption. *Matematicheskaia teoriia igr i ee prilozheniia*, 2010, vol. 2, no. 4, pp. 106-119 (in Russian).

29. Ugol'nitskii G. A., Usov A. B. Vertical coalitions in hierarchical three-level control systems of fan-like structure. *Journal of Computer and Systems Sciences International*, 2010, vol. 49, no. 6, pp. 923-930.

30. 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).

31. Dettmer H. W. *Goldratt's theory of constraints: a systems approach to continuous improvement*. ASQ Quality Press, 1997.

32. Algazin G. I. *Ekologo-ekonomicheskie s razlichnoi informirovannost'iu uchastnikov: modeli, mekhanizmy funktsionirovaniia, otsenki effektivnosti* [Ecological and economic awareness with a variety of parties: models, mechanisms and effectiveness evaluation]. Barnaul, Altai State University, 1997 (in Russian).

33. Algazin G. I. *Modeli sistemnogo kompromissa v sotsial'no-ekonomicheskikh issledovaniiakh: monografiia* [The models of system compromise in socio-economic research. Monograph]. Barnaul, Azbuka Publ., 2009. 239 p. (in Russian).

34. Algazin G. I. Methodological aspects of mathematical researching of conflicts in the modern organizational systems theories. *Izvestiya of Altai State University*, 2001, no. 1, pp. 7-9 (in Russian).

35. Zhukovskii V. I., Kudriavtsev K. N. *Uravnoveshivanie konfliktov i prilozheniia* [Balancing conflicts and applications]. Moscow, URSS Publ., 2012. 304 p. (in Russian).

36. Zhukovskii V. I., Zhukovskaia L. V. *Risk v mnogokriterial'nykh i konfliktnykh sistemakh pri neopredelennosti. Monografiia* [The risk in multi-criteria and conflicting systems under uncertainty. Monograph]. Moscow, URSS Publ., 2004. 267 p. (in Russian).

37. Sysoev D. V. Conditions of formation of the conflict in the given systems.

Nauchnyi vestnik Voronezhskogo gosudarstvennogo arkhitekturno-stroitel'nogo universiteta. Seriia: Informatsionnye tekhnologii v stroitel'nykh, sotsial'nykh i ekonomicheskikh sistemakh, 2013, no. 1, pp. 41-48 (in Russian).

38. Sysoev V. V., Sysoev D. V. Action of the System. *Sistemy upravleniia i informatsionnye tekhnologii*, 2005, vol. 18, no. 1, pp. 51-58 (in Russian).

39. Sysoev V. V. *Opredelenie konflikta funktsioniruiushchikh sistem // Matematicheskoe modelirovanie tekhnologicheskikh system* [The definition of the conflict of systems]. Collection of scientific papers. Voronezh, Voronezh State Technological Academy, 1996. pp. 3-9 (in Russian).

40. Sysoev V. V. *Konflikt. Sotrudnichestvo. Nezavisimost'. Sistemnoe vzaimodeistvie v strukturno-parametricheskom predstavlenii* [Conflict. Cooperation. Independence. System interaction in structural-parametric representation]. Moscow, Moscow Academy of Economics and Law, 1999. 151 p. (in Russian).

41. Sysoev V. V. Modelirovanie struktury konflikta funktsioniruiushchikh sistem [Modeling of the structure of the conflict of systems]. *Collection of scientific papers – "Informatsionnye tekhnologii i sistemy"*, Voronezh, Voronezh State Technological Academy, 1995, pp. 6-7 (in Russian).

42. Rubinshtein M. I. *Optimal'naia gruppirovka vzaimosviazannykh obektov* [Optimal grouping of related objects]. Moscow, Nauka Publ., 1989. 168 p. (in Russian).

43. Koriagin M. E. *Optimizatsiia upravleniia gorodskimi passazhirskimi perevozkami na osnove konfliktno-ustoichivykh reshenii. Dissertatsiia dokt. tekhn. nauk* [Optimization of management of urban passenger transport on the basis of conflict-sustainable solutions. Dr. habil. Tesis]. Novokuznetsk, Kuzbass State Technical University, 2011. 345 p. (in Russian).

44. Koriagin M. E. *Ravnovesnye modeli sistemy gorodskogo passazhirskogo transporta v usloviiakh konflikta interesov* [The equilibrium model of urban passenger transport in terms of conflict of interest]. Novosibirsk, Nauka Publ., 2011. 140 p. (in Russian).

45. 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).

46. Guseinov B. A., Ushakov I. A. *Optimal'noe raspredelenie resursov v territorial'nykh sistemakh* [The optimal allocation of resources in the territorial systems]. Moscow, Dorodnicyn Computing Centre RAS, 1985. 52 p. (in Russian).

47. Mistrov L. E. Fundamentals of the organizational- functional synthesis methodology for complex systems. *Instruments and Systems: Monitoring, Control, and Diagnostics*, 2006, no. 12, pp. 56-61 (in Russian).

48. Mistrov L. E. Metod analiticheskogo resheniia zadachi sistemotekhnicheskogo sinteza konfliktno-ustoichivykh obespechivaiushchikh funktsional'nykh organizatsionno-tekhnicheskikh system [Method, analytical solutions to system integrators synthesis konfliktno-sustainable providing functional organizational-engineering systems]. *Mashinostroitel*, 2005, no. 1, pp. 25-33 (in Russian).

49. Bukharin S. N., Tsyganov V. V. *Metody i tekhnologii informatsionnykh voin* [Methods and techniques of information warfare]. Moscow, Akademicheskii Proekt Publ., 2007. 382 p. (in Russian).

50. Rastorguev S. P., Litvinenko M. V. *Informatsionnye operatsii v seti Internet* [Information operations on the Internet]. Moscow, Center for strategic assessments and forecasts, 2014. 128 p. (in Russian).

51. Alfyorov A. G., Belitsky A. M., Stepanets Yu. A., Tolstykh N. N. Infocommunicational system control interception. *Teoriia i tekhnika radiosviazi*, 2014, no. 4, pp. 5-13 (in Russian).

52. 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).

53. Nikolskii B. A. *Osnovy teorii sistem i kompleksov radioelektronnoi bor'by* [Fundamentals of the theory of systems and complexes of electronic warfare]. Samara, Samara national research University named after academician S.P. Korolev, 2012. 174 p. (in Russian).

54. Makarenko S. I. Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression. *Systems of Control, Communication and Security*, 2015, no. 3, pp. 122-185. Available at: http://journals.intelgr.com/sccs/archive/2015-03/07-Makarenko.pdf (accessed 23 August 2016) (in Russian).

55. Novikov D. A. Hierarchical models of combat. *Upravlenie bol'simi sistemami*, 2012, no. 37, pp. 25-62 (in Russian).

56. Ashkenazy V. O. *Primenenie teorii igr v voennom dele* [Application of game theory in the military]. Moscow, Sovetskoe Radio Publ, 1961. 362 p. (in Russian).

57. Druzhinin V. V., Kontorov D. S. *Voprosy voennoi sistemotekhniki* [The questions of military engineering]. Moscow, Voenizdat Publ., 1976. 224 p. (in Russian).

58. Druzhinin V. V., Kontorov A. S., Kontorov D. S. *Vvedenie v teoriiu konflikta* [Introduction to the theory of conflict]. Moscow, Radio i Sviaz Publ., 1989. 288 p. (in Russian).

59. Voronov E. M. *Metody optimizatsii upravleniia mnogoob"ektnymi mnogokriterial'nymi sistemami na osnove stabil'no-effektivnykh igrovykh reshenii* [Optimization methods for the control of multi-object multi-criteria systems on the basis of stable-effective gaming solutions]. Moscow, Bauman Moscow State Technical University, 2001. 576 p. (in Russian).

60. Vladimirov V. I., Vladimirov I. V. *Osnovy otsenki konfliktno-ustoichivykh 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).

61. 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).

62. Vakin S. A., Shustov L. N. *Osnovy radioprotivodeistviia i radiotekhnicheskoi razvedki* [The basics of jamming and electronic reconnaissance]. Moscow, Sov. Radio Publ., 1968. 448 p. (in Russian).

63. 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).

64. Druzhinin V. V., Kontorov D. S. *Konfliktnaia radiolokatsiia* [Conflict radar]. Moscow, Radio i Sviaz Publ., 1982. 288 p. (in Russian).

65. Paliy A. I. *Radioelektronnaia bor'ba* [Electronic warfare]. Moscow, Voenizdat Publ., 1989. 350 p. (in Russian).

66. Tsvetnov V. V., Demin V. P., Kupriianov A. I. *Radioelektronnaia bor'ba: radiorazvedka i radioprotivodeistvie* [Electronic warfare: radio reconnaissance and countermeasure]. Moscow, Moscow Aviation Institute (National Research University), 1998. 248 p. (in Russian).

67. Tsvetnov V. V., Demin V. P., Kupriianov A. I. *Radioelektronnaia bor'ba: radiomaskirovka i pomekhozashchita* [Electronic warfare: radioactive and jamming protection]. Moscow, Moscow Aviation Institute (National Research University), 1999. 240 p. (in Russian).

68. 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).

69. 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).

70. Kuprijanov A. I. *Radioelektronnaia bor'ba* [Electronic warfare]. Moscow, Vuzovskaia Kniga Publ., 2013. 360 p. (in Russian).

71. Perunov Ju. M., Fomichev K. I., Iudin L. M. *Radioelektronnoe podavlenie informatsionnykh kanalov sistem upravleniia oruzhiem* [Electronic suppression of information channels of weapon control systems]. Moscow, Radiotekhnika Publ., 2003. 416 p. (in Russian).

72. 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).

73. Radzievskii V. G. Metod obosnovaniia kharakteristik signalo-podobnykh izluchenii v konfliktnoi radiolokatsii [Method of the substantiation of the characteristics of signal-like radiation in a conflict radar]. *Radiotekhnika*, 2000, no. 6, pp. 53-58 (in Russian).

74. Radzievskiy V. G. and etc. *Sovremennaia radioelektronnaia bor'ba. Voprosy metodologii* [Modern electronic warfare. Methodological issues]. Moscow, Radiotekhnika Publ., 2006. 424 p. (in Russian).

75. Sukhorukov Ju. S., Shliakhin V. M. Konfliktno-igrovaia model'

radiolokatsionnogo obnaruzheniia tselei v usloviiakh protivodeistviia [Conflict-game model of radar target detection in the face of opposition]. *Radiotekhnika*, 1991, no. 9, pp. 44-59 (in Russian).

76. Sukhorukov Ju. S, Shliakhin V. M. Printsipy modelirovaniia dinamiki vzaimodeistviia storon v usloviiakh radiolokatsionnogo konflikta [Principles of modelling the dynamics of interaction between the parties in terms of radar conflict]. *Radiotekhnika*, 1992, no. 1-2, pp. 4-11 (in Russian).

77. 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).

78. Shliakhin V. M., Karkotskii V. L., Iakovlev Ju. V. Konfliktno-obuslovlennye vyigryshi storon v usloviiakh protivodeistviia [Conflict-due to the winnings of the parties in the face of opposition]. *Radiotekhnika*, 1992, no. 7-8, pp. 3-6 (in Russian).

79. Shliakhin V. M., Iakovlev Ju. V. Kontrradiopodavlenie [Counter-radio countermeasure]. *Radioelectronics and Communications Systems*, 2004, vol. 47, no. 4, pp. 3-13 (in Russian).

80. Merkulov V. I., Chernov V. S., Drogalin V. V., Kanashchenkov A. I., Samarin O. F., Alekseev Ju. Ia., Gromov M. V., Dudnik P. I., Zhiburtovich N. Ju., Ilchuk A. R., Rodzivilov V. A., Slukin T. P., Fedorov I. B., Frantsev V. V., Chernov M. V., Shuklin A. I. *Pomekhozashchishchennost' radiolokatsionnykh sistem. Sostoianie i tendentsii razvitiia* [Noise immunity of radar systems. Status and trends of development]. Moscow, IPRZhR Publ., 2003. 464 p. (in Russian).

81. Melnikov Ju. P. *Vozdushnaia radiotekhnicheskaia razvedka (metody otsenki effektivnosti)* [Aerial electronic reconnaissance (methods of assessment of effectiveness)]. Moscow, Radiotekhnika Publ., 2005. 304 p. (in Russian).

82. Mironov V. A., Radzievskii V. G. Osobennosti navigatsionno-vremennogo obespecheniia radioelektronnykh sistem v usloviiakh konflikta [Features navigatsionno-time maintenance of electronic systems in conflict]. *Radiotekhnika*, 1998, no. 6, pp. 4-9 (in Russian).

83. Mironov V. A., Radzievskii V. G. Pomekhozashchishchennost' apparatury radioinertsial'nogo navigatsionnogo kompleksa s adaptivnoi antennoi reshetkoi [The noise immunity of the equipment radionavigating navigation system with adaptive antenna array]. *Radiotekhnika*, 1999, no. 6, pp. 79-82 (in Russian).

84. Mironov V. A. Metodicheskie osnovy issledovaniia effektivnosti funktsionirovaniia apparatury potrebitelei sputnikovykh sistem navigatsionno-vremennogo obespecheniia v usloviiakh radioelektronnogo konflikta [Methodological foundations for research of efficiency of functioning of user equipment of satellite navigation and time support in conditions of radio-electronic conflict]. *Radiotekhnika*, 2010, no. 6, pp. 87-90 (in Russian).

85. Diatlov A. P., Kulbikaian B. Kh. *Radiomonitoring izluchenii sputnikovykh radionavigatsionnykh sistem. Monografiia* [The radiation spectrum monitoring of satellite navigation systems. Monograph]. Moscow, Radio i Sviaz Publ., 2006. 270 p. (in Russian).

86. Diatlov A. P., Diatlov P. A., Kulbikaian B. Kh. *Radioelektronnaia bor'ba so sputnikovymi radionavigatsionnymi sistemami. Monografiia* [Electronic warfare satellite radio navigation systems. Monograph]. Moscow, Radio i Sviaz Publ., 2004. 226 p. (in Russian).

87. Vartanesian V. A. *Radioelektronnaia razvedka* [Signals intelligence]. Moscow, Voenizdat Publ., 1991. 254 p. (in Russian).

88. Demin V. P., Kupriianov A. I., Sakharov A. V. *Radioelektronnaia razvedka i radiomaskirovka* [Electronic reconnaissance and radioactive]. Moscow, Moscow Aviation Institute (National Research University), 1997. 155 p. (in Russian).

89. Radzievskii V. G., Sirota A. A. *Informatsionnoe obespechenie radioelektronnykh sistem v usloviiakh konflikta* [Information support of electronic systems in conflict]. Moscow, IPRZR Publ., 2001. 456 p. (in Russian).

90. Radzievskii V. G., Sirota A. A. *Teoreticheskie osnovy radioelektronnoi razvedki* [The theoretical basis of electronic intelligence]. 2 edition. Moscow, Radiotekhnika Publ., 2004. 432 p. (in Russian).

91. Radzievskii V. G., Sirota A. A. Bazovye statisticheskie modeli protsessa radiotekhnicheskoi razvedki v khode protivodeistviia radiolokatsionnym sredstvam [The basic statistical model for a process surveillance during the anti-radar means]. *Radiotekhnika*, 1992, no. 1-2, pp. 24-31 (in Russian).

92. Radzievskii V. G., Sirota A. A. Osobennosti sinteza algoritmov obrabotki informatsii pri analize sostoianiia slozhnykh radioelektronnykh ob"ektov protivodeistviia [Features of synthesis of algorithms for processing information in the analysis of complex electronic object counter]. *Informatsionnyi konflikt v spektre elektromagnitnykh voln*, 1994, pp. 4-13 (in Russian).

93. Sirota A. A., Borisov Ju. A. Algoritmy fil'tratsii pri postuplenii oshibochnykh i protivorechivykh dannykh v kanalakh nabliudeniia sistem sbora i obrabotki informatsii [Filtering when receiving incorrect and inconsistent data in channels surveillance collection systems and processing of information]. *Radiotekhnika*, 1997, no. 6, pp. 51-57 (in Russian).

94. Sirota A. A. Veroiatnostnye modeli formirovaniia rezul'tiruiushchego vektora nabliudenii v mnogourovnevykh, mnogopozitsionnykh sistemakh [Probabilistic models generate the result vector of the observations in multilevel, multiposition systems]. *Radiotekhnika*, 1998, no. 6, pp. 10-14 (in Russian).

95. Sirota A. A., Borisov Ju. A. Granitsy dlia tochnostnykh kharakteristik fil'trov otsenivaniia v usloviiakh chastichnoi skrytnosti nabliudaemykh ob"ektov [Bounds for the accuracy characteristics of the filters estimation under conditions of partial secrecy of the observed objects]. *Sintez, peredacha i priem signalov upravleniia i sviazi*, 1997, no. 4, pp. 59-66 (in Russian).

96. Levashova T. V. Principles of ontology management used in the knowledge integration environment. *SPIIRAS Proceedings*, 2002, vol. 2, no. 1, pp. 51-68 (in Russian).

97. Dvornikov S. V. *Teoreticheskie osnovy chastotno-vremennogo analiza kratkovremennykh signalov. Monografiia* [Theoretical foundations of time-frequency analysis short-time signals. Monograph]. Saint-Petersburg, Military Academy of

Communications, 2010. 240 p. (in Russian).

98. Koziratsky Ju. L., Erofeev A. N., Sokolovskii S. P. Model' konfliktnogo vzaimodeistviia “narushitel - podsistema 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).

99. Lenshin A. V. Bortovye sistemy i kompleksy radioelektronnogo podavleniia [Onboard systems and complexes of radio-electronic suppression]. Voronezh, Nauchnaia Kniga Publ., 2014. 590 p. (in Russian).

100. Diatlov A. P., Kulbikaian B. Kh. *Korreliatsionnaia obrabotka shirokopolosnykh signalov v avtomatizirovannykh kompleksakh radiokontrolia. Monografiia* [Correlation Processing of Wideband Signals in Automated Complexes of radio. Monograph]. Moscow, Goriachaia liniia – telikom Publ., 2013. 332 p. (in Russian).

101. Rembovskii A. I., Ashikhmin A. V., Koz'min V. A. *Radiomonitoring - zadachi, metody, sredstva. 2 izd* [Radio Monitoring - Targets, Methods, Tools. 2nd edition]. Moscow, Goriachaia liniia - Telekom Publ., 2010. 624 p. (in Russian).

102. Menshakov Ju. K. *Vidy i sredstva inostrannykh tekhnicheskikh razvedok* [Forms and Means of Foreign Technical Intelligence]. Moscow, Bauman Moscow State Technical University Publ., 2009. 656 p. (in Russian).

103. Menshakov Ju. K. *Osnovy zashchity ot tekhnicheskikh razvedok* [Fundamentals of Protection Against Technical Intelligence]. Moscow, Bauman Moscow State Technical University Publ., 2011. 487 p. (in Russian).

104. Lifanov Ju. P. Sablin V. N., Saltan M. I. *Napravleniia razvitiia zarubezhnykh sredstv nabliudeniia nad polem boia* [Development Trends of Foreign Funds Observe the Battlefield]. Moscow, Radiotekhnika Publ., 2004. 64 p. (in Russian).

105. Vakulenko A. A., Verba B. C., Dod V. N. Organization of conflict-sustainable management of the integrated electronic system in the dynamics of the conflict with the means of jamming. *Radiotekhnika*, 2006, no. 1, pp. 50-53 (in Russian).

106. Grebeniuk V. L., Isaev V. V., Melnikov V. F. Optimizing asset management interference in the tripartite conflict with the means of signals intelligence and information transmission system. *Informatsionno-izmeritelnye i upravlyayushchie sistemy*, 2009, vol. 7, no. 9, pp. 42-48 (in Russian).

107. Khoreev A. A. *Tekhnicheskie sredstva i sposoby promyshlennogo shpionazha* [Technical Means and Methods of Industrial Espionage]. Moscow, ZAO «Dalsnab» Publ., 1997. 230 p. (in Russian).

108. Kuprijanov A. I., Saharov A. V. Shevtsov V. A. *Osnovy zashchity informatsii* [The basics of information security]. Moscow, Publishing center «Akademia», 2006. 256 p. (in Russian).

109. Averchenkov V. I., Rytov M. Ju., Kuvyklin A. V., Gainulin T. R. *Metody i sredstva inzhenerno-tekhnicheskoi zashchity informatsii. Uchebnoe posobie*

[Methods and Means of Technical Protection of Information]. Moscow, FLINTA Publ., 2011. 187 p. (in Russian).

110. Chukliaev I. I., Morozov A. V., Bolotin I. B. *Teoreticheskie osnovy optimal'nogo postroeniia adaptivnykh sistem kompleksnoi zashchity informatsionnykh resursov raspredelennykh vychislitel'nykh sistem: monografiia* [Theoretical Foundations of Optimal Construction of Adaptive Systems of Comprehensive Protection of Information Resources Distributed Computing Systems. Monograph] Smolensk, Military Academy of Army Air Defence Publ., 2011. 227 p. (in Russian).

111. Goldshtein B. S., Kriukov Ju. S., Pinchuk A. V., Khegai I. P., Shliapoberskii V. E. *Interfeisy SORM. Spravochnik* [The System interfaces technical means to ensure the operational-search activities]. Sankt-Peterburg, BKhV-Peterburg Publ., 2006. 160 p. (in Russian).

112. Devianin P. N. *Modeli bezopasnosti komp'iuternykh system* [Models for computer security]. Moscow, Publishing center «Akademia», 2005. 144 p. (in Russian).

113. Pakhomova A. S., Pakhomov K. A., Razinkin K. A. To the problem of the development of a structural model of computer intelligence. *Informatsiia i bezopasnost*, 2013, vol. 16. no. 1, pp. 115-118 (in Russian).

114. Bugrov Ju. G., Pakhomova A. S., Baburin A. V. Utochnenie tekhnologicheskoi skhemy komp'iuternoi razvedki s uchetom klassifikatsii komp'iuternykh atak i vozmozhnostei vredonosnykh sredstv [Clarification of the technological scheme of computer intelligence based classification of computer attacks and malicious tools capabilities]. *Informatsiia i bezopasnost*, 2014, vol. 17. no. 2, pp. 292-295 (in Russian).

115. Privalov A. A. *Metod topologicheskogo preobrazovaniia stokhasticheskikh setei i ego ispol'zovanie dlia analiza sistem sviazi VMF* [The method of topological transformations of stochastic networks and its application to the analysis of communication systems of the Navy]. Saint-Petersburg, Naval Academy, 2000. 166 p. (in Russian).

116. Ziuko A. G. *Pomekhoustoichivost' i effektivnost' sistem sviazi* [Noise immunity and efficiency of communication systems]. Moscow, Sviaz Publ., 1972. 359 p. (in Russian).

117. 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 Sviaz Publ., 1981. 267 p. (in Russian).

118. 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 Sviaz Publ., 1985. 264 p. (in Russian).

119. Borisov V. I., Zinchuk V. M. *Pomekhozashchishchennost' sistem radiosviazi. Veroiatnostno-vremennoi podkhod* [Noise immunity of radio communication systems. Probabilistic-temporal approach]. Moscow, Radio i Sviaz

Publ., 1999. 252 p. (in Russian).

120. 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).

121. Vladimirov V. I. *Printsipy i apparat sistemnykh issledovanii radioelektronnogo konflikta* [The principles and apparatus of the electronic system studies conflict]. Voronezh, Voronezh Higher Military Engineering College of Radioelectronics, 1992 (in Russian).

122. 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).

123. Vladimirov V. I., Gostev V. A. *Osnovy radiopodavleniia, postroeniia i primeneniia sredstv i kompleksov REP sistem peredachi informatsii. Tom 2. Kurs lektsii* [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).

124. Vladimirov V. I. *Sistemy i kompleksy REB. Tom 1: Sistemotekhnicheskie osnovy postroeniia* [Systems and electronic warfare systems. Tom 1: Systems Engineering Fundamentals of Building]. Voronezh, Military Engineering College of Radioelectronics, 1999 (in Russian).

125. Vladimirov V. I. *Informatsionnye osnovy radiopodavleniia 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).

126. Semisoshenko M. A. *Upravlenie avtomatizirovannymi setiami dekametrovoi sviazi v usloviiakh 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).

127. Chudnov A. M. *Analiz pomekhozashchishchennosti linii i setei sviazi* [Analysis of noise immunity of lines and communication networks]. Leningrad, Military Communications Academy, 1988. 34 p. (in Russian).

128. Chudnov A. M. *Pomekhoustoichivost' linii i setei sviazi v usloviiakh optimizirovannykh pomekh* [Interference resistance lines and communication networks under conditions optimized interference]. Leningrad, Military Communications Academy, 1986. 84 p. (in Russian).

129. Barashkov P. N., Rodimov A. P., Tkachenko K. A., Chudnov A. M. *Model' sistemy sviazi s upravliaemymi strukturami v konfliktnykh usloviiakh* [Model of communication system with controlled structures in conflict settings]. Leningrad,

Military Communications Academy, 1986. 52 p. (in Russian).

130. Burachenko D. L. *Optimal'noe razdelenie tsifrovykh signalov mnogikh pol'zovatelei v liniiakh i setiakh sviazi v usloviiakh 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).

131. Karatuev M. I. Vzaimodeistvie sil i sredstv razvedki i ognevogo porazheniia v operatsii [The interaction of forces and means of reconnaissance and fire damage in the operation]. Military Thought, 1998, no. 6, pp. 37-41 (in Russian).

132. Kuznetsov V. I. *Radiosviaz' v usloviiakh radioelektronnoi bor'by* [Radio communication electronic warfare conditions]. Voronezh, Voronezh Research Institute of Communications, 2002, 403 p. (in Russian).

133. Bogovik A. V., Ignatov V. V. *Effektivnost' sistem voennoi sviazi i metody ee otsenki* [The effectiveness of military communications systems and assessment methods]. Saint-Petersburg, Military Communications Academy, 2006. 183 p. (in Russian).

134. Isakov E. E. *Ustoichivost' voennoi sviazi v usloviiakh 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).

135. Odoevskii 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).

136. 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 Radiosviazi*, 2010, no. 2, pp. 37-43 (in Russian).

137. 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 Radiosviazi*, 2010, no. 2, pp. 44-49 (in Russian).

138. 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).

139. Shabalin E. A., Milov V. R. Network Resources Allocation with Information Value Consideration in Case of Electromagnetic Blanketing. *Informatsionno-izmeritelnye i upravlyayushchie system*, 2008, no. 11, pp. 87-93 (in Russian).

140. 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).

141. 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).

142. Tolstykh N. N., Pavlov V. A., Vorobeva E. I. *Vvedenie v teoriiu 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).

143. Budnikov S. A. Model of a generalized conflict, radio-electronic means. *Radiotekhnika*, 2008, no. 11, pp. 8-10 (in Russian).

144. 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).

145. Boyko A. A., D'iakova A. V. The Method of Development of Test Remote Information-Technical Impacts on the Spatial Distribution of Information-Technical Equipment. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 3, pp. 84-92 (in Russian).

146. Boiko A. A. Method of Analytical Modeling of Spread of Viruses in Computer Networks with Different Structures. *SPIIRAS Proceedings*, 2015, vol. 42, no. 5, pp. 196-211 (in Russian).

147. Maltsev G. N., Pankratov A. N., Lesniak D. A. Probabilistic Characteristics of Information System Security Changes under Unauthorized Access. *Informatsionno-upravliaiushchie sistemy*, 2015, no. 1, pp. 50-58 (in Russian).

148. Maltsev G. N., Telichko V. V. Optimization of Information Protection Means in the Informational-Command System with Wireless Channels Access Based on Threats Realiza-tion Graph. *Informatsionno-upravliaiushchie sistemy*, 2008, no. 4, pp. 29-33 (in Russian).

149. Biriukov D. N., Lomako A. G. The synthesis method preemption scenarios based on associative and reflex behavior. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2015, no. 1, pp. 52-56 (in Russian).

150. Biryukov D. N., Rostovtsev Yu. G. Approach to creation of the consistent theory of synthesis scenarios of anticipatory behavior in the conflict. *SPIIRAS Proceedings*, 2015, no. 1, pp. 94-111 (in Russian).

151. Biryukov D. N., Lomako A. G. Podkhod k postroeniiu IB-sistem, sposobnykh sintezirovat' stsenarii 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).

152. Eremeev M. A., Lomako A. G., Ovcharov V. A., Akulov S. A., Korotkov V. P., Svergun N. V. Adaptive Control Method of active network equipment of the telecommunications network in terms of computer attacks. *Informatsionnoe protivodeistvie ugrozam terrorizma*, 2012, no. 19. pp. 136-146 (in Russian).

153. 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).

154. 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).

155. Morozov A. V., Chukliaev I. I. Informatsionnaia bezopasnost' vychislitel'nykh sistem boevogo upravleniia v aspekte informatsionnogo protivoborstva. *Problemy bezopasnosti rossiiskogo obshchestva*, 2013, no. 2-3. pp. 85-90 (in Russian).

156. Morozov A. V., Maiburov D. G., Chukliaev I. I. Information security of computer systems of command and control in the aspect of information warfare. *Problemy bezopasnosti rossiiskogo obshchestva*, 2014, no. 2, pp. 177-183 (in Russian).

157. Starodubtsev Ju. I., Bukharin V. V., Semenov S. S. Tekhnosfernaia voina [Techno War]. *Military Thought*, 2012, no. 7. pp. 22-31 (in Russian).

158. Starodubtsev Ju. I., Bukharin V. V., Semenov S. S. Technospherny war. *Informatsionnye sistemy i tekhnologii*, 2011, no. 1, pp. 80-85 (in Russian).

159. 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).

160. 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).

161. Griniaev S. N. *Sistemy obnaruzheniia vtorzhenii i reagirovaniia na komp'iuternye intsidenty na osnove mobil'nykh programm-agentov* [Intrusion detection systems, and responding to computer incidents based mobile software agents]. Moscow, Center for strategic assessments and forecasts Publ., 2005. 46 p. (in Russian).

162. Starodubtsev Ju. I., Bukharin V. V., Kir'ianov A. V., Balenko O. A. Security Assessment Method Information And Telecommunications Networks From Destructive Effects Software. *Vestnik komp'iuternykh i informatsionnykh tekhnologii*, 2013, vol. 106, no. 4, pp. 37-42. (in Russian).

163. Bukharin V. V., Kir'ianov A. V., Starodubtsev Ju. I. A method of protecting information networks against cyber attacks. *Trudy MAI*, 2012, no. 57, pp. 16 (in Russian).

164. Starodubtsev Ju. I., Eryshov V. G., Korsunskii A. S. Process Model of information security monitoring in the information and telecommunication systems. *Automation of Control Processes*, 2011, no. 1, pp. 58-61 (in Russian).

165. Sheluhin O. I., Sakalema D. Zh., Filinova A. S. *Obnaruzhenie vtorzhenii v komp'iuternye seti (setevye anomalii)* [Intrusion detection in computer networks (network anomalies)]. Moscow, Goriachaia liniia - Telekom Publ., 2013. 220 p. (in Russian).

166. Kotsyniak M. A., Kuleshov I. A, Lauta 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).

167. Kotsyniak M. A., Osadchii A. I., Kotsyniak M. M., Lauta O. S., Dement'ev V. E., Vasiukov D. Ju. *Obespechenie ustoichivosti informatsionno-telekommunikatsionnykh sistem v usloviiakh 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).

168. 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).

169. Ostapenko G. A. Strukturno-parametricheskaia model' informatsionnogo konflikta system [Structural-parametric model of the information conflict systems]. *Bezopasnost Informatsionnykh Tekhnology*, 2007, no. 2, pp. 93-94 (in Russian).

170. Ostapenko G. A. *Informatsionnye operatsii i ataki v sotsiotekhnicheskikh sistemakh. Monografiia* [Information Operations and Attacks in Socio-Technical Systems. Monograph]. Voronezh, Voronezh State Technical University, 2005. 204 p. (in Russian).

171. Jotsov V. S., Sgurev V. S., Yusupov R. M., Khomonenko A. D. The Ontology for the Semantic Conflicts Resolution. *SPIIRAS Proceedings*, 2008, no. 7, pp. 26-40.

172. Emelin V. I. *Metody i modeli otsenki i obespecheniia informatsionnoi bezopasnosti avtomatizirovannykh sistem upravleniia kriticheskimi sistemami Diss. ... dokt. tekhn. nauk.* [Methods and Models of Assessment and Information Security Critical Systems Automated Control Systems. Extended Abstract of D.Sc. Thesis]. Saint-Petersburg, SPIIRAN, 2012. 239 p. (in Russian).

173. Bukharin S. N. Tsyganov V. V. *Metody i tekhnologii informatsionnykh voin* [Methods and technologies of information warfare]. Moscow, Akademicheskii Proekt Publ., 2007. 382 p. (in Russian).

174. 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).

175. Gorbachev I. E., Anikanov G. A. Approach to reduce the risk of functioning disorganization of critical infrastructure in the information conflict. *Information Security Problems. Computer Systems*, 2015, no. 2, pp. 106-119 (in Russian).

176. Popovskii V. V., Lemeshko A. V., Evseeva O. Ju. Dynamic resource management TCS: mathematical models in the state space. *Naukovi zapiski UNDIZ*, 2009, vol. 9, no. 1, pp. 3-26 (in Russian).

177. Aizeks R. *Differentsial'nye igry* [Differential Games]. Moscow, Mir Publ., 1967. 480 p. (in Russian).

178. Pontriatin L. S. *K teorii differentsial'nykh igr* [By the Theory of Differential Games]. *Uspekhi Matematicheskikh Nauk*, 1966, vol. 21, no. 4. pp. 219-

274 (in Russian).

179. Krasovskii N. N., Subbotin A. I. *Pozitsionnye differentsial'nye igry* [Positional Differential Games]. Moscow, Nauka Publ., 1974. 456 p. (in Russian).

180. Petrosian L. A *Differentsial'nye igry presledovaniia* [Differential Pursuit Games] Leningrad, Leningrad State Universaty Publ., 1977. 224 p. (in Russian).

181. Nikolaev V. I., Tolstykh N. N. Adaptivnoe, situatsionnoe i refleksivnoe upravlenie podsistemoi zashchity informatsii avtomatizirovannykh telekommunikatsionnykh kompleksov [Adaptive, situational and reflective control subsystem of information protection of automated telecommunication complexes]. *Radio Communication Theory and Equipment*, 2006, no. 2, pp. 79-87 (in Russian).

182. Tolstykh N. N., Piatunin A. N., Mareichenko I. V., Pavlov V. A., Slepov I. Iu. Printsipy rannego obnaruzheniia priznakov konfliktnogo rezhima vzaimodeistviia avtomatizirovannykh telekommunikatsionnykh kompleksov [The principles of early detection of signs of conflict interaction mode automated telecommunication complexes]. *Radio Communication Theory and Equipment*, 2004, no. 2, pp. 115 (in Russian).

183. Smol'iakov E. R. *Teoriia konfliktnykh ravnovesii* [The Theory of Conflict Equilibria]. Moscow, URSS Publ., 2005 (in Russian).

184. Blagodatskikh A. I., Petrov N. N. Group pursuit with state constraints in Pontryagin's almost periodic example. *Differential Equations*, 2015, vol. 51, no. 3, pp. 391-398 (in Russian).

185. Yuditskiy S. A. A technique for graph-dynamic modeling of binary games based on scenario bindings. *Large-scale Systems Control*, 2010, no. 31, pp. 289-298 (in Russian).

186. Yuditskiy S. A. Structural-machine model of conflict solutions in organizational systems. *Large-scale Systems Control*, 2008, no. 23, pp. 126-136 (in Russian).

187. Novikov D. A. *Setevye struktury i organizatsionnye sistemy* [Network structure and organizational system]. Moscow, Institute of Control Sciences RAS, 2003. 102 p. (in Russian).

188. Novikov D. A. *Mekhanizmy funktsionirovaniia mnogourovnevykh organizatsionnykh system* [Mechanisms of functioning of multilevel organizational systems]. Moscow, Fond "Problemy upravleniia" Publ., 1999. 161 p. (in Russian).

189. Nguen Kuang Tkhyong. *Metody i modeli nadezhnosti, effektivnosti i bezopasnosti slozhnykh tekhnicheskikh sistem v konfliktnykh situatsiiakh. Dis. ... d-ra tekhn. nauk.* [Methods and Models of Reliability, Efficiency and Safety of Complex Technical Systems in Conflict Situations. Extended Abstract of Dr. Sc. Thesis]. Tver, 1999. 322 p. (in Russian).

190. Taran T. A. *Logicheskie metody i modeli podderzhki priniatiia reshenii v konfliktnykh situatsiiakh. Dis. ... d-ra tekhn. nauk.* [Logic Methods and Models of Decision Support in Conflict Situations. Extended Abstract of Dr. Sc. Thesis]. Moscow, 1998. 266 p. (in Russian).

191. Borisov A. N., Korneeva G. V. The linguistic approach to building decision models under uncertainty. *Metody priniatiia reshenii v usloviiakh*

neopredelennosti, Riga Polytechnic Institute Publ., 1980, pp. 4-12 (in Russian).

192. Borisov A. N., Alekseev A. V. *Obrabotka nechetkoi informatsii v sistemakh priniatiia reshenii* [Fuzzy Information Processing in the Decision-Making Systems]. Moscow, Radio i Sviaz Publ., 1989. 304 p. (in Russian).

193. Borisov A. N., Krumberg O. A., Fedorov I. P. *Priniatie reshenii na osnove nechetkikh modelei: Primery ispol'zovaniia* [Decision-Making Based on Fuzzy Models, Examples of Use]. Riga, Zinatne Publ., 1990. 184 p. (in Russian).

194. Smirnov Ju. A. *Radiotekhnicheskaia razvedka* [Radio Intelligence]. Moscow, Voenizdat Publ., 2001. 456 p. (in Russian).

195. Alekseev A. A. *Chastotno-vremennoi analiz signalov sviazi i radiotekhnicheskogo obespecheniia* [Time-Frequency Analysis of Signals and Radio Support]. Leningrad, Military Academy of Communications, 1987 (in Russian).

196. Chelyshev V. D., Iakimovets V. V. *Radioelektronnye sistemy organov administrativnogo i voennogo upravleniia. Ch. 1* [Radio-electronic system of administrative bodies and military control. Part 1]. Saint-Petersburg, Military Academy of Communications, 2006. 456 p. (in Russian).

197. Marchuk L. A. *Prostranstvenno-vremennaia obrabotka signalov v liniiakh radiosviazi* [The Space-Time Signal Processing in Radio Communications]. Leningrad, Military Communications Academy, 1991. 136 p. (in Russian).

198. Dvornikov S. V., Zhelezniak V. K., Komarovich V. F., Khramov R. N. Metod obnaruzheniia radiosignalov na osnove obrabotki ikh chastotno-vremennykh raspredelenii plotnosti energii [Radio Detection Method Based On The Processing Of Time-Frequency Distribution Of The Energy Density]. *Informatsiia i kosmos*, 2005, no. 4, pp. 13-16 (in Russian).

199. Dvornikov S. V., Alekseeva T. E. Raspredelenie Alekseeva i ego primenenie v zadachakh chastotno-vremennoi obrabotki signalov [Distribution Alekseeva and its application to problems of time-frequency signal processing]. *Informatsiia i kosmos*, 2006, no. 3, pp. 9-21 (in Russian).

200. Zakharchenko A. N., Veselov Ju. G., Ostrovskii A. S., Selvesiuk N. I., Adaptive for application conditions and current tasks method of estimating technical state of digital optoelectronic systems. *Informatika i sistemy upravleniia*, 2015, vol. 44, no. 5, pp. 33-44 (in Russian).

201. Kononov V. I. *Teoreticheskie osnovy radio- i radiotekhnicheskoi razvedki* [Theoretical Bases of Radio and Electronic Intelligence]. Saint-Petersburg, Military Academy of Communications, 2000 (in Russian).

202. Zamarin A. I., Atakishchev O. I., Tavalinskii D. A., Riumshin K. Iu. Postdetector technical analysis of digital identifikavyh sequences with complex structures. *Proceedings of the South-West State University*, 2014, vol. 52, no. 1, pp. 14-21 (in Russian).

203. Zamarin A. I., Tavalinskii D. A. Generalized model of building redundancy reduction procedures of reporting. *Informatsiia i kosmos*, 2004, no. 5. pp. 52-74 (in Russian).

204. Saiapin V. N., Dvornikov S. V., Simonov A. N., Volkov R. V. Metod prostranstvenno-vremennoi fil'tratsii signalov na osnove antennykh reshetok

proizvol'noi prostranstvennoi konfiguratsii [Method of spatio-temporal filtering on the basis of signals of antenna array arbitrary spatial configuration]. *Informatsiia i kosmos*, 2006, no. 3, pp. 83-89 (in Russian).

205. Komarovich V. F., Saenko I. B. Komp'iuternye informatsionnye voiny kontseptsiia i realii [Computer information warfare concept and realities]. *Zashchita informatsii*. *Konfident*, no. 4-5, 2002, pp. 84-88 (in Russian).

206. Ilin A. P., Shakin N. K. K voprosu o meste radioelektronnoi razvedki, radioelektronnoi bor'by i radioelektronnoi maskirovki v informatsionnoi bor'be [To a question about the place of electronic intelligence, electronic warfare and electronic masking information in the fight against]. *Military Thought*, 2008, no. 1, pp. 25-30 (in Russian).

207. Myrova L. O., Chepizhenko A. Z. *Obespechenie stoikosti apparatury sviazi k ioniziruiushchim i elektromagnitnym izlucheniiam. 2-e izd* [Ensuring Stability of Communications Equipment to the Ionizing and Electromagnetic Radiation. 2nd edition]. Moscow, Radio i Sviaz' Publ., 1988. 296 p. (in Russian).

208. Dobykin V. D., Kupriianov A. I., Ponomarev V. G., Shustov L. H. *Radioelektronnaia bor'ba. Silovoe porazhenie radioelektronnykh sistem* [Electronic Warfare. Power Failure of Electronic Systems]. Moscow, Vuzovskaia Kniga Publ., 2007. 468 p. (in Russian).

209. Akbashev B. B., Baliuk N. V., Kechiev L. N. *Zashchita ob"ektov telekommunikatsii ot elektromagnitnykh vozdeistvii* [Protection of Telecommunications Facilities from Electromagnetic Influences]. Moscow, Grifon Publ., 2014. 472 p. (in Russian).

210. Gizatullin R. M., Gizatullin Z. M. *Pomekhoustoichivost' i informatsionnaia bezopasnost' vychislitel'noi tekhniki pri elektromagnitnykh vozdeistviiakh po seti elektropitaniia. Monografiia* [Immunity and Information Security of Computer Technology with Electromagnetic Effects on the Power Supply. Monograph]. Kazan, Kazan State Technical University, 2014. 142 p. (in Russian).

211. Mikhailov V. A. *Razrabotka metodov i modelei analiza i otsenki ustoichivogo funktsionirovaniia bortovykh tsifrovykh vychislitel'nykh kompleksov v usloviiakh prednamerennogo vozdeistviia sverkhkorotkikh elektromagnitnykh izluchenii Diss. ... dokt. tekhn. nauk.* [Development of Methods and Models of Analysis and Evaluation of the Sustainable Functioning of the Onboard Digital Computer Complexes in the Conditions of the Deliberate Influence of Ultrashort Electromagnetic Radiation Extended Abstract of Dr. Sc. Thesis]. Moscow, «Argon» Research Institute, 2014. 390 p. (in Russian).

212. Mikheev O. V. *Sredstva izmerenii i metody ispytanii telekommunikatsionnykh sistem v usloviiakh vozdeistviia elektromagnitnykh impul'sov s subnanosekundnoi dlitel'nost'iu fronta Diss. ... kand. tekhn. nauk.* [The Measuring and Test Methods Telecommunication Systems under the Impact of Electromagnetic Pulses with Sub-Nanosecond Rise Time. Extended Abstract of Ph.D. Thesis]. Moscow, HSE Moscow Institute of Electronics, 2006. 162 p. (in Russian).

213. Hohlov N. S., Sidorov A. V. Estimation of radio communication and

control system resistance to destructive electromagnetic effect. *Vestnik of Volga State University of Technology. Series Radio Engineering and Infocommunication Systems*, 2013, vol. 18, no. 2, pp. 27-35 (in Russian).

214. Sidorov A. V. *Otsenka ustoichivosti sredstv radiosviazi i upravleniia organov vnutrennikh del k destruktivnym elektromagnitnym vozdeistviiam. Diss. ... kand. tekhn. nauk.* [Assessment of the Stability of Radio Communication and Management of the Internal Affairs Bodies to Destructive Electromagnetic Impacts. Extended Abstract of Ph.D. Thesis]. Voronezh, Voronezh Institute of MIA of Russia, 2015. 149 p. (in Russian).

215. Iakushin S. P. *Metody i sredstva otsenki vozdeistviia elektromagnitnogo impul'sa bol'shoi energii na telekommunikatsionnye seti. Diss. ... kand. tekhn. nauk.* [Methods and Tools for Assessing the Impact of High Energy Electromagnetic Pulse on Telecommunication Networks]. Moscow, HSE Moscow Institute of Electronics, 2004. 146 p. (in Russian).

216. Klimov S. M. *Metody i modeli protivodeistviia komp'iuternym atakam* [Methods and models for countering computer attacks]. Liubertsy, Katalist Publ., 2008. 316 p. (in Russian).

217. Klimov S. M., Sychev M. P., Astrakhov A. V. *Protivodeistvie komp'iuternym atakam. Metodicheskie osnovy* [The combat computer attacks. Methodological foundations]. Moscow, Bauman Moscow State Technical University, 2013. 108 p. (in Russian).

218. Belonozhkin V. I., Ostapenko G. A. *Informatsionnye aspekty protivodeistviia terrorizmu* [Informational aspects of counter-terrorism]. Moscow, Goriachaia liniia – Telekom Publ., 2009. 112 p. (in Russian).

219. Deshina A. E., Bursa M. V., Ostapenko A. G., Kalashnikov A. O., Ostapenko G. A. *Upravlenie informatsionnymi riskami mul'tiservernykh sistem pri vozdeistvii DDOS-atak* [Information risk management for multi-server systems under the influence of DDOS-attacks]. Voronezh, Nauchnaia Kniga Publ., 2014. 160 p. (in Russian).

220. Butuzov V. V., Bursa M. V., Ostapenko A. G., Kalashnikov A. O., Ostapenko G. A. *Informatsionnye riski flud-atakuemykh komp'iuternykh system* [Information risks of flood the attacked computer systems]. Voronezh, Nauchnaia Kniga Publ., 2015. 160 p. (in Russian).

221. Radko N. M., Skobelev I. O. *Risk-modeli informatsionno-telekommunikatsionnykh sistem pri realizatsii ugroz udalennogo i neposredstvennogo dostupa* [The risk model of information and telecommunication systems in the implementation of threats with remote and direct access]. Moscow, RadioSoft Publ., 2011. 229 p. (in Russian).

222. Iazov Iu. K., Serdechnyi A. L., Baburin A. V. Metod formalizatsii protsessa nesanktsionirovannogo dostupa v informatsionnykh sistemakh, postroennykh s ispol'zovaniem sredstv virtualizatsii, osnovannyi na matematicheskom apparate setei Petri [The method of the formalization process of unauthorized access to information systems, built using virtualization, based on the mathematical formalism of Petri nets]. *Informatsiia i bezopasnost*, 2013, vol. 16,

no. 4. pp. 518-521 (in Russian).

223. Agranovskii A. V., Repalov S. A., Khadi R. A., Iakubets M. B. O nedostatkakh sovremennykh sistem obnaruzheniia vtorzhenii [On the shortcomings of modern intrusion detection systems]. *Telekommunikatsii*, 2005, no. 1, pp. 39. (in Russian).

224. Agranovskii A. V., Khadi R. A. Novyi podkhod k zashchite informatsii - sistemy obnaruzheniia komp'iuternykh ugroz [A new approach to data security - computer threats detection system]. *Vestnik Rossiiskogo fonda fundamental'nykh issledovanii*, 2007, no. 4, pp. 22 (in Russian).

225. Agranovskii A. V., Khadi R. A., Iakubets M. B. Statisticheskie metody obnaruzheniia anomal'nogo povedeniia v sistemakh obnaruzheniia atak [Statistical Methods for the Detection of Abnormal Behavior in Intrusion Detection Systems]. *Informatsionnye tekhnologii*, 2005, no. 1, pp. 18 (in Russian).

226. Maliuk A. A. *Informatsionnaia bezopasnost': kontseptual'nye i metodologicheskie osnovy zashchity informatsii* [Information Security: Conceptual and Methodological Framework for the Protection of Information]. Moscow, Goriachaia Liniia -Telekom Publ., 2004. 280 p. (in Russian).

227. Isupov A. B. *Modelirovanie protsessa funktsionirovaniia telekommunikatsionnoi seti v usloviiakh programmno-apparatnykh vozdeistvii* [Modelling of Telecommunication Network Operation Process in Terms of Software and Hardware Effects]. *Polythematic online scientific journal of Kuban State Agrarian University*, 2012, no. 81. pp. 103-114 (in Russian).

228. Isupov A. B. *Mnogourovnevyi bionicheskii algoritm dlia obnaruzheniia i identifikatsii programmno-apparatnykh vozdeistvii na informatsionno-telekommunikatsionnye seti* [Multilevel Bionic Algorithm for Detection and Identification of Hardware and Software Impact on Information and Telecommunication Network]. *Polythematic online scientific journal of Kuban State Agrarian University*, 2012, no. 81, pp. 76-92 (in Russian).

229. Privalov A. A., Popov P. V. Elektromagnitnaia sovmestimost' sredstv sviazi i ee vliianie na ustoichivost' funktsionirovaniia sistemy sviazi VMF v usloviiakh vozdeistviia protivnika oruzhiem funktsional'nogo porazheniia [Electromagnetic compatibility of communication and its influence on stability of functioning of communication systems of the Navy under the impact of the enemy weapons for functional defeat]. *Technologies of electromagnetic compatibility*, 2004, no. 4, pp. 65-68 (in Russian).

230. Privalov A. A., Popov P. V. Elektromagnitnaia sovmestimost' sredstv sviazi i ee vliianie na ustoichivost' funktsionirovaniia sistemy sviazi VMF v usloviiakh vozdeistviia protivnika oruzhiem funktsional'nogo porazheniia [Electromagnetic compatibility of communication and its influence on stability of functioning of communication systems of the Navy under the impact of the enemy weapons for functional defeat]. *Technologies of electromagnetic compatibility*, 2004, no. 11, pp. 65-67 (in Russian).

231. Adadurov S. E., Elishev V. V., Efimov V. P. *Problemy peredachi informatsii v mnogosputnikovykh setevykh sistemakh* [Problems of information

transmission in multi-satellite network systems]. Moscow, The Ministry of Defence, 1996. 120 p. (in Russian).

232. Adadurov S. E., Astanin A. V., Maltsev G. N., Riazanov S. N., Stepanov M. G. and etc. *Modelirovanie setevykh sputnikovykh sistem peredachi informatsii* [Simulation of network of satellite communication systems]. Moscow, The Ministry of Defence, 1996. 125 p. (in Russian).

233. Peregudov M. A., Boyko A. A. Model Procedure of Random Multiple Access to the Environment Type S-ALOHA. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 6, pp. 75-81 (In Russian).

234. Griniaev S. N. *Intellektual'noe protivodeistvie informatsionnomu oruzhiiu* [Intellectual opposition to arms information]. Moscow, SINTEG Publ., 1999. 232 p. (in Russian).

235. Prilepskii 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).

236. Levin V. I. Logical-Algebraic Approach to Conflicts Modeling. *Systems of Control, Communication and Security*, 2015, no. 4, pp. 69-87 (in Russian).

237. Levin V. I. Avtomatnoe modelirovanie istoricheskikh protsessov na primere voin [Automata Modeling of Historical Processes on The Example of Wars]. *Radio Electronics, Computer Science, Control*, 2002, no. 3, pp. 93-101 (in Russian).

238. Levin V. I. Automaton Modeling of Processes of Formation and Splitting of Collectives. *Cybernetics and Systems Analysis*, 2003, vol. 39, no. 3, pp. 394-401 (in Russian).

239. 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).

240. 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).

241. Ukhin A. L., Koziratsky Ju. L. Veroiatnostnaia model' konflikta radioelektronnykh sistem upravleniia i telekommunikatsii v usloviiakh 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).

242. Koziratsky Ju. L., Kuschev S. S., Chernuho 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).

243. Tarasov A. A. *Funktsional'naia otkazoustoichivost' sistem obrabotki informatsii*. *Monografiia* [Functional fault-tolerant information processing systems. Monograph]. Moscow, Moscow Institute of new information technologies of The

Federal security service of the Russian Federation, 2009. 181 p. (in Russian).

244. Zhumatii 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).

245. 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).

246. 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).

247. 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).

248. Kotenko I. V., Saenko I. B., Polubelova O. V., Chechulin A. A. Technologies of security information and event management for computer network protection. *Information Security Problems. Computer Systems*, 2012, no. 2, pp. 57-68 (in Russian).

249. 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).

250. Vyalykh A. S., Vyalykh S. A., Sirota A. A. Algoritm analiza nadezhnosti programmnogo obespecheniia informatsionnykh sistem v usloviiakh vnutrennikh uiazvimostei i negativnykh vozdeistvii [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).

251. 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).

252. Alferov A. G., Tolstykh I. O., Tolstykh N. N., Pozdysheva O. V., Mordovin A.I. Ustochivost' infokommunikatsionnykh sistem v usloviiakh 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).

253. Styugin M. A. Statement of the problem of misinformation in information systems. *Informatsionnye voiny*, 2014, vol. 31, no. 3, pp. 6-11 (in Russian).

254. Styugin M. A. Methods to achieve information superiority in conflict systems. *Informatsionnye voiny*, 2013, vol. 27, no. 3, pp. 17-21 (in Russian).

255. Styugin M. A. The is reflexive-signature analysis of conflicts. *Scientific and Technical Information Processing*, 2012, no. 2, pp. 39-50 (in Russian).

256. Styugin M. A. Action planning in the conflict at functional structure level. *Informatsionnye voiny*, 2009, no. 2, pp. 16-21 (in Russian).

257. 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).

258. Novikov S. N. *Metodologiia zashchity pol'zovatel'skoi informatsii na osnove tekhnologii setevogo urovnia mul'tiservisnykh setei sviazi* [Methodology of protection of user information based on the network level multiservice communication networks]. Moscow, Goriachaia Liniia - Telekom, 2015. 128 p. (in Russian).

259. 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).

260. 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).

261. Grigorev V. R., Shurkin L. O. Setetsentricheskie voiny s pozitsii sinergetiki [Setetsentricheskie voiny with pozitsii sinergetiki]. *Vestnik Rossiiskogo gosudarstvennogo gumanitarnogo universiteta*, 2014, no. 11, pp. 67-100 (in Russian).

262. Parshutkin A. V. Conceptual interconnection model of conflict information and telecommunication systems. *Voprosy kiberbezopasnosti*, 2014, vol. 8, no. 5, pp. 2-6 (in Russian).

263. 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 Seriia*, 2015, no. 5-6, pp. 13-17 (in Russian).

264. Isaev V. V., Babusenko S. I. Statisticheskoe modelirovanie mnogoproletnykh setei paketnoi radiosviazi [Statistical modeling of multi-span networks, packet radio]. *Tekhnika sredstv sviazi: materialy 18 nauchno-tekhnicheskoi konferentsii* [Proceedings of the 18th scientific and technical conference "Technique of communication"], Voronezh, Research Institute of telecommunications, 1992 (in Russian).

265. Babusenko S. I., Isaev V. V. Analiticheskaia model' marshrutizatsii v paketnoi seti [Analytical model of routing in a packet network]. *Tekhnika sredstv sviazi: materialy 18 nauchno-tekhnicheskoi konferentsii* [Proceedings of the 18th scientific and technical conference "Technique of communication"], Voronezh, Research Institute of telecommunications, 1992 (in Russian).

266. Babusenko S. I. Model protsessa radiopodavleniia paketnoi radioseti s protokolom nenastoichivogo dostupa s proslushivaniem nesushchei [The process model of the jamming packet radio network Protocol nenastoychiv access with listening of carrier]. *Proceedings of 31 military-scientific conference of the Academy*. Leningrad, Military Academy of Communications, 1990 (in Russian).

267. Zima V. M., Kotukhov M. M., Lomako A. G., Markov A. S., Moldovian A. A. Razrabotka sistem informatsionno-komp'iuternoi bezopasnosti [The development systems information and computer security]. Saint-Petersbirg, Mozhaisky Military Space Academy, 2003. 327 p. (in Russian).

268. Alferov A. G., Mordvin A. I., Tolstyh N. N., Pozdysheva O. V. Spectacular relationshio management systems with limited resources sa a news conflict. *Information and security*, 2014, vol. 17, no. 4, pp. 548-557 (in Russian).

269. Tsaregorodtsev A. V. *Metody, modeli i algoritmy sinteza zashchishchennykh informatsionnykh system* [Methods, models and algorithms for the synthesis of protected information systems]. Moscow, Russian state tax Academy of the Ministry of Finance of the Russian Federation, 2009. 207 p. (in Russian).

270. Tsaregorodtsev A. V. Organizatsiia zashchity ob"ektov informatizatsii ot silovykh destruktivnykh elektromagnitnykh vozdeistvii [Organization of protection of objects of Informatization from the forceful destructive electromagnetic impacts]. National Security / nota bene, 2011, no. 3, pp. 139-152 (in Russian).

271. Tsaregorodtsev A. V. Recommendations for information objects protection from the electromagnetic destructive effects. *Modern Science: actual problems of theory and practice. Series of "Natural and Technical Sciences"*, 2012, no. 4-5, pp. 38-48 (in Russian).

272. Voskobovich V. V., Mikhailov V. A., Myrova L. O., Tsaregorodtsev A. V. Systematic Approach to development of the Methodology of infocommunication systems Analysis and Evaluation of Resistance to Destructive electromagnetic effects. Technologies of electromagnetic compatibility, 2012, no. 1, pp. 51-58 (in Russian).

273. 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, pp. 2. Available at: http://jre.cplire.ru/jre/jun12/9/text.pdf (accessed 26 August 2016) (in Russian).

274. 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 26 August 2016) (in Russian).

275. Grechishnikov E. V., Gorelik S. P., Dobryshin M. M. Support way of required security of a communication network against external destructive influences. *Telekommunikatsii*, 2015, no. 6, pp. 30-37 (in Russian).

276. Grechishnikov E. V., Belov A. S., Shumilin V. S. Sposob upravleniia zashchishchennost'iu setei sviazi v usloviiakh destruktivnykh programmnykh vozdeistvii [The method of controlling the security of communication networks in terms of destructive software impacts]. *Telekommunikatsii*, 2014, no. 3, pp. 18-22 (in Russian).

277. Grechishnikov E. V., Gorelik S. P., Belov A. S. Predlozheniia po obespecheniiu zhivuchesti elementov setei sviazi v chrezvychainykh situatsiiakh [Proposals to ensure the durability of the elements of communication networks in emergency situations]. *Telekommunikatsii*, 2013, no. 4, pp. 23-26 (in Russian).

278. Grechishnikov E. V., Gusev A. P. Obespechenie ustoichivosti sistemy sviazi v usloviiakh sverkhvysokochastotnogo elektromagnitnogo izlucheniia [Sustainability of the communication system in the conditions of microwave electromagnetic radiation]. *Telekommunikatsii*, 2011, no. 10, pp. 37-41 (in Russian).

279. Kotenko D. I., Kotenko I. V., Saenko I. B. Methods and tools for attack modeling in large computer networks: state of the problem. *SPIIRAS Proceedings*, 2012, vol. 22, no. 3, pp. 5-30 (in Russian).

280. Kotenko I. V., Saenko I. B. Developing the system of intelligent services to protect information in cyber warfare. *SPIIRAS Proceedings*, 2012, vol. 22, no. 3, pp. 84-100 (in Russian).

281. Kotenko I. V., Saenko I. B. Architecture of the system of intelligent information security services in critical infrastructures. *SPIIRAS Proceedings*, 2013, vol. 24, no. 1, pp. 21-40 (in Russian).

282. Zegzhda D. P., Kovalenko S. L. Security issues of wireless networks IEEE 802.11a/b/g. *Information Security Problems. Computer Systems*, 2006, no. 2, pp. 45-49 (in Russian).

283. Zegzhda D. P., Korotich A. V. Control of Access to Information Resources of Information Telecommunication Systems with the High Availability. *Naukoemkie tekhnologii*, 2007, vol. 7, no. 11, pp. 41-46 (in Russian).

284. Zegzhda P. D. General trends of information security technologies evolution in the epoch of information warfare. *Information Security Problems. Computer Systems*, 2007, no. 1, pp. 60-72 (in Russian).

285. Mikhailov R. L. *Pomekhozashchishchennost' transportnykh setei sviazi spetsial'nogo naznacheniia. Monografiia* [Noise immunity of transport networks for special purposes. Monograph]. Cherepovets, The Cherepovets higher military engineering school of radio electronics, 2016. 128 p. (in Russian).

286. Vavilov V. A., Nazarov A. A. Issledovanie ustoichivykh setei mnozhestvennogo dostupa s istochnikom povtornykh vyzovov, funktsioniruiushchim v sluchainoi srede [Study sustainable networks multiple access with a source of repeated calls operating in random environment]. *Computational Technologies*, 2008, vol. 13, no. 5, pp. 14-18 (in Russian).

287. Vishnevsky V. M., Lyahov A. I. Estimation of Productivity of the Off-Wire Network Under Noses. *Automation and Remote Control*, 2000, no. 12, pp. 87-103 (in Russian).

288. Elesin M. E., Khodarevskii D. N. Analiticheskaia model' vliianiia veroiatnosti oshibki v radiokanale na kharakteristiki paketnoi peredachi seti besprovodnogo dostupa [An analytical model of the influence of the error probability in the radio channel on the characteristics of packet wireless access network]. *Aktual'nye problemy razvitiia tekhnologicheskikh sistem gosudarstvennoi okhrany, spetsial'noi sviazi i spetsial'nogo informatsionnogo obespecheniia: VIII Vserossiiskaia mezhvedomstvennaia nauchnaia konferentsiia: materialy i doklady* [VIII all-Russian interdepartmental scientific conference "actual problems of development of technological systems of state protection, special communications and special information support"]. Orel, Academy of Federal security service of

Russia, 2013, pp. 36-40 (in Russian).

289. Kovalkov D.A. The dynamic analysis of the radio channel of the random access of the communication system with the spread spectrum and relaying of the signals. *Infokommunikacionnye tehnologii*, 2009, vol. 7, no. 1, pp. 23-29 (in Russian).

290. Osipov D. S. On the performance of a non-coherent DHA FH OFDMA system with threshold reception under jamming. *Informatsionno-upravliaiushchie sistemy*, 2010, no. 6, pp. 28-32 (in Russian).

291. Spirina E. A. Optimizatsiia raspredeleniia informatsii v fiksirovannykh setiakh shirokopolosnogo radiodostupa s uchetom vnutrisistemnykh pomekh [Optimization of data distribution in fixed broadband wireless access networks subject to interference]. *Journal of radio electronics*, 2015, no. 9. Available at: http://jre.cplire.ru/jre/sep15/5/text.pdf (accessed 26 August 2016) (in Russian).

292. Chakrian V. R. *Mnogomernye stokhasticheskie i imitatsionnye modeli teletrafika i kanalov peredachi dannykh v usloviiakh pomekh. Dis. ... kand. tekhn. nauk* [Multidimensional stochastic and simulation models of teletraffic and data channels in noise conditions. Extended Abstract of Ph.D. Thesis]. Rostov-na-Donu, 2009. 157 p. (in Russian).

293. Popovskii V. V., Volotka V. S. Metody analiza dinamicheskikh struktur telekommunikatsionnykh sistem [Methods of analysis of dynamic structures of telecommunication systems]. *Eastern-European Journal of Enterprise Technologies*, 2013, vol. 65, no. 5/2, pp. 18-22 (in Russian).

294. Popovskii V. V., Volotka V. S. Matematicheskoe modelirovanie nadezhnosti infokommunikatsionnykh sistem [Mathematical modelling of secure information and communication systems]. *Telekomunikacijni ta informacijni tehnologii'*, 2014, no. 3, pp. 5-9 (in Russian).

295. Popovskii V. V., Lemeshko A. V., Mel'nikova L. I., Andrushko D. V. Obzor i sravnitel'nyi analiz osnovnykh modelei i algoritmov mnogoputevoi marshrutizatsii v mul'tiservisnykh telekommunikatsionnykh setiakh [Basic models and algorithms of multipath routing for multi-service telecommunication networks]. *Prikladnaia radioelektronika*, 2005, vol. 4, no. 4, pp. 372-382. Available at: http://alem.ucoz.ua/_ld/0/10_Lemeshko_PRE_20.pdf (accessed 01 May 2015) (in Russian).

296. Lemeshko A. V., Evseeva O. Yu., Drobot O. A. The Method of Paths Independents Choice with Definition of their Quantity at the Solving of Multipath Routing Problem. *Praci UNDIRT*, 2006, vol. 48, no. 4, pp. 69-73. Available at: http://alem.ucoz.ua/_ld/0/14_Lemeshko_UNIIRT.pdf (accessed 01 May 2015) (in Russian).

297. Lemeshko O. V., Kozlova H. V., Romanyuk A. O. A Mathematical Model of Fault-tolerant Routing, Presented Algebraic Equations of MPLS-Network State. *Systemy obrobky informacii'*, 2013, vol. 109, no. 2, pp. 217-220 (in Russian).

298. Popkov V. K. *Mathematical Models of Connection*. Novosibirsk, ICM&MG SB RAS Publ., 2006. 490 p. (in Russain).

299. Popkov V. K., Blukke V. P., Dvorkin A. B. Modeli analiza ustoichivosti i zhivuchesti informatsionnykh setei [Model analysis the sustainability and

survivability of information networks]. *Problems of informatics*, 2009, no. 4, pp. 63-78 (in Russian).

300. Sorokin A. A., Dmitriev V. N. Description of Communication Systems with Dynamic Network Topology by Means of Model "Flickering" Graph. *Vestnik of Astrakhan State Technical University. Series: Management, Computer science and Informatics*, 2009, no. 2. pp. 134-139 (in Russian).

301. Sorokin A. A., Dmitriev V. N., Tran Quoc Toan, Reznikov P. S. Evaluation of the Results of Using the RIP Protocol in Communication Systems with Dynamic Network Topology Using Simulation Method. *Vestnik of Astrakhan State Technical University. Series: Management, Computer science and Informatics*, 2014, no. 4, pp. 85-93 (in Russian).

302. Perepelkin D. A. Algoritm parnykh perestanovok marshrutov na baze protokola OSPF pri dinamicheskom otkaze uzlov i linii sviazi korporativnoi seti [The algorithm of pairwise permutations of routes for OSPF Protocol under condition dynamic failure of nodes and communication lines network]. *Vestnik Riazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*, 2014, vol. 47, no. 1, pp. 84-91 (in Russian).

303. Perepelkin D. A. Algoritm adaptivnoi uskorennoi marshrutizatsii na baze protokola IGRP pri dinamicheskom otkaze uzlov i linii sviazi korporativnoi seti [The algorithm is adaptive accelerated routing for IGRP Protocol under condition dynamic failure of nodes and communication lines network]. *Vestnik Riazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*, 2012, vol. 42, no. 4, pp. 33-38 (in Russian).

304. Perepelkin D. A. Dynamic Corporate Network Structure and Communication Links Loading Formation Based on Routes Pairs Permutations Data. *Informatsionnye tekhnologii*, 2014, no. 4, pp. 52-60 (in Russian).

305. Koriachko V. P., Perepelkin D. A. *Analiz i proektirovanie marshrutov peredachi dannykh v korporativnykh setiakh* [Analysis and design of routes of transmission of data in corporate networks]. Moscow, Goriachaia liniia – Telekom Publ., 2012. 236 p. (in Russian).

306. Meikshan V. I. Analysis of Equipment Faults Influence on Performance of Multiservice Network with Adaptive Routing. *Proceedings of the Russian higher school academy of sciences*. 2010, vol. 15, no 2, pp. 69-80 (in Russian).

307. Gorev P. G., Nazarov A. S., Pasechnikov I. I. Opredelenie sviaznosti v putevom prostranstve sostoianii telekommunikatsionnoi seti [The definition of connectivity in the route state-space telecommunication network]. *Tambov University reports. Series: Natural and Technical sciences*, 2012, vol. 17, no. 5, pp. 1360-1363 (in Russian).

308. Litvinov K. A., Pasechnikov I. I. Podkhody k resheniiu zadachi marshrutizatsii v sovremennykh telekommunikatsionnykh sistemakh [The routing problem in modern telecommunication systems]. *Tambov University reports. Series: Natural and Technical sciences*, 2013. vol. 18, no. 1, pp. 64-69 (in Russian).

309. Gromov Ju. Ju., Drachev V. O., Nabatov K. A., Ivanova O. G. *Sintez i analiz zhivuchesti setevyh sistem: monografija* [Synthesis and Analysis Net Systems

Reliability]. Moscow, Mashinostroenie-1 Publ., 2007, 152 p. (in Russian).

310. Kovalkov D. A. Matematicheskie modeli otsenki nadezhnosti mul'tiservisnogo uzla dostupa [Mathematical model for reliability evaluation of multi-service access node network]. *Radio and telecommunication systems*, 2011, no. 2, pp. 64-71 (in Russian).

311. Gorbunov I. E. Metodologiia analiza i sinteza rekonfiguriruemykh topologii mobil'noi sviazi [The methodology of analysis and synthesis of reconfigurable topologies for mobile communication]. *Matematychni mashyny i systemy*, 2006, no. 2, pp. 48-59 (in Russian).

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

313. Lastovchenko M. M., Zubareva E. A., Sachenko V. O. Metod analiza effektivnosti rekonfiguratsii topologii postroeniia besprovodnykh mul'tiservisnykh setei povyshennoi pomekhozashchishchennosti [The method of analysis of efficiency of reconfiguration of the topology construction of wireless multi-service networks high noise immunity]. *Upravliaiushchie sistemy i mashiny*, 2009, no. 6, pp. 79-86 (in Russian).

314. Stromov A. V., Nechaev Yu. B., Baev A. D. Simulation of routing in wireless mesh network with adaptation to the impact of several interference sources. *Radio Communication Theory and Equipment*, 2014, no. 4, pp. 46-52 (in Russian).

315. Tsimbal V. A., Toiskin V. E., Iakimova I. A., Kosareva L. N. Nakhozhdenie granits primenimosti protokola TSR v setiakh sviazi s nizkoskorostnymi kanalami [Finding the limits of applicability of TCP in networks with low speed channels]. *XXIII Vserossiiskaia nauchno-tekhnicheskaia konferentsiia* [XXIII all-Russian scientific-technical conference]. Serpukhov, Military Academy of strategic Missile forces named after Peter the Great (Branch), 2014, pp. 290-259 (in Russian).

316. Toiskin V. E., Tsimbal V. A., Iakimova I. A., Kabanovich S.G. Markovskaia model' dovedeniia mnogopaketnykh soobshchenii po steku protokolov TCP/IP s protseduroi «skol'ziashchee okno» [Markov model of communicating multi-packet messages, the Protocol stack TCP/IP procedure "sliding window"]. *International conference RES-2014*. Moscow, Russian scientific-technical society of radio engineering, electronics and communication named after A.S. Popov, 2014, pp. 112-114 (in Russian).

317. Svintsov A. A., Solodukha R. A. Analiticheskaia model' funktsionirovaniia linii peredachi dannykh s reshaiushchei obratnoi sviaz'iu i okonnym upravleniem potokom v usloviiakh vozdeistviia pomekh [An analytical model of the operation of the transmission with decision feedback and window flow control in conditions of interference]. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia*, 2007, no. 2, pp. 197-202 (in Russian).

318. Mikhailov R. L., Makarenko S. I. Estimating Communication Network Stability under the Conditions of Destabilizing Factors Affecting it. *Radio and telecommunication systems*, 2013, no. 4, pp. 69-79 (in Russian).

319. Makarenko S. I., Mikhailov R. L., Novikov E. A. Issledovanie kanal'nykh i setevykh parametrov kanala sviazi v usloviiakh 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 1 Aug 2016) (in Russian).

320. Makarenko S. I. Convergence Time of IGP Routing Protocol. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 45-98. Available at: http://sccs.intelgr.com/archive/2015-02/03-Makarenko.pdf (accessed 1 Aug 2016) (in Rissian).

321. Makarenko S. I., Mikhaylov R. L. The Model of Functioning of the Router in the Case of Limited Reliability of Communication Canals. *Infocommunikacionnye tehnologii*, no. 2, 2014, pp. 44-49 (in Russian).

322. Makarenko S. I., Ryimshin K. Yu., Mixajlov R. L. 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).

323. 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://sccs.intelgr.com/archive/2015-01/07-Makarenko.pdf (accessed 1 Aug 2016) (in Rissian).

324. Vlasov J. B., Nikolayev V. I., Tolstykh I. O., Tolstykh N. N., Chelajdinov J. V. Estimated potential threat of the dataflow in the info communication system. *Radiotekhnika*, 2012, no. 8, pp. 33-40 (in Russian).

325. Makarenko S.I. Premeditated formation of the traffic of difficult structure due to implementation in the communication system of additional imitative traffic. *Voprosy kiberbezopasnosti*, 2014, vol. 4, no. 3, pp. 7-13 (In Russian).

326. Ushanev K. V. Simulation Models of Queuing Systems of Type Pa/M/1, H_2/M/1 and Research on the Basis of their Quality of Service Traffic with a Complicated Structure. *Systems of Control, Communication and Security*, 2015, no. 4, pp. 217-251. Available at: http://journals.intelgr.com/sccs/archive/2015-04/14-Ushanev.pdf (accessed 26 August 2016) (in Russian).

327. 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).

328. Makarenko S. I., Chucklyaev I. I. The terminological basis of the informational conflict area. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 13-21 (in Russian).

329. Gurevich I. M. Mnogourovnevaia model' seti sviazi [Multi-level model of the communication network]. *Voprosy kibernetiki. Protokoly i metody kommutatsii v vychislitel'nykh setiakh*, 1986, pp. 72-88 (in Russian).

330. Abramenkov 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).

331. Gurevich I. M. Dinamicheskaia model' seti sviazi [The dynamic model of the communication network]. *Teoriia teletrafika v sistemakh informatiki*, 1989, pp. 77-86 (in Russian).

332. 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).

333. Vakulenko A. A., Shevchuk V. I. Matematicheskaia 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).

334. 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).

335. Popovskiy V. V., Lemeshko A. V., Evseeva O. Ju. Matematicheskie modeli telekommunikatsionnykh sistem. Chast' 1. Matematicheskie modeli funktsional'nykh svoistv 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).

336. Semenova I. I., Mishurin A. O. Management system model of information counterforce. *Vestnik Saratov State Technical University*, 2010, vol. 4, no. 1, pp. 150-160 (in Russian).

337. Veselov G. E., Kolesnikov A. A. Synergetics approach to integrated security of complex system. *Izvestiya SFedU. Engineering Sciences*, 2012, vol. 129, no. 4, pp. 8-18 (in Russian).

338. Iakovlev V. B., Kolesnikov A. A. Sinergeticheskoe upravlenie nelineinymi ob"ektami s khaoticheskoi dinamikoi. *Izvestiya SFedU. Engineering Sciences*, 2001, vol. 23, no. 5, pp. 126-131 (in Russian).

339. Bazykin A. D. *Nelineinaia dinamika vzaimodeistvuiushchikh populiatsii* [Nonlinear dynamics of interacting populations]. Moskva, Institute of computer science, 2003. 368 p. (in Russian).

340. Kotenko I. V., Ulanov A. V. Komandy agentov v kiberprostranstve: modelirovanie protsessov zashchity informatsii v global'nom Internete [Teams of agents in cyberspace: modeling processes of information security on the global Internet]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk*, 2006, vol. 27, pp. 108-129 (in Russian).

341. Kotenko I. V., Ulanov A. V. Komp'iuternye voiny v internete:

modelirovanie protivoborstva programmnykh agentov [Computer wars on the Internet: modeling warfare software agents]. *Zasita informacii. Inside*, 2007, vol. 16, no. 4, pp. 38-45 (in Russian).

342. Kotenko I. V., Ulanov A. V. Multiagent simulation of protection of information resources in Internet. *Journal of Computer and Systems Sciences International*, 2007, vol. 46, no. 5, pp. 741-755.

343. Vaipan S. N., Vakulenko A. A., Verba V. S., Yagolnikov S. V. Estimation Factors for Conflict Stability of Radio Electronic Functioning Under Conditions of Information Opposition Used for Checking of Applied Technical Solutions. *Radiotekhnika*, 2006, no. 1, pp. 46-49 (in Russian).

344. Vakulenko A. A., Shevchuk V. I., Yagolnikov S. V. Otsenka effektivnosti radioelektronnoi sistemy v dinamike konflikta [Evaluation of the effectiveness of electronic systems in the dynamics of conflict]. *Radiotekhnika*, 2009, no. 9, pp. 84-86 (in Russian).

345. Vlasov V. V., Shevchuk V. I., Shevchuk D. V., Yagolnikov S. V. Metod for synthesis of space sounding for Earth under conditions of the complex information conflict. *Radiotekhnika*, 2015, no. 3, pp. 57-63 (in Russian).

346. Vakulenko A. A., Verba V. S., Dod V. N. Organization of Conflict - Stable Control for a Multifunctional Integrated Radio Electronic System in Dynamics of Conflict with Means of Radio Electronic Suppression. *Radiotekhnika*, 2006, no. 1, pp. 50-53 (in Russian).

347. Nikolaev V. I., Tolstyh N. N., Alferov A. G., Stepanets Yu. A., Tolstyh I. O., Roldugin N. G., Artemov M. V. Forced synthesis of processor facility's specified goal state: concept of control interception. *Radiotekhnika*, 2016, no. 5. pp. 84-96 (in Russian).

348. Verba V. S., Demin A. N., Khripunov S. P. Principles of the Construction of the System of the Prognostication of the development of the Conflict Situations. *Radiotekhnika*, 2010, no. 8. pp. 20-25 (in Russian).

349. Merkulov V. I., Dobykin V. D., Drogalin V. V. Funktsional'noe porazhenie radioelektronnykh sistem [Functional defeat of radio-electronic systems]. *Fazotron*, 2006, no. 3, pp. 4 (in Russian).

350. Drogalin V. V., Kazakov V. D., Merkulov V. I. Prednamerennye algoritmicheskie vozdeistviia na tsifrovye vychislitel'nye sistemy aviatsionnykh radiolokatsionnykh sistem [Intentional algorithmic impact on digital computing systems, aircraft radar systems]. *Fazotron*, 2007, no. 1, pp. 2 (in Russian).

351. Merkulov V. I., Zabelin I. V. Traektornoe upravlenie nabliudeniem kak sposob sozdaniia prednamerennykh algoritmicheskikh vozdeistvii na radiolokatsionnye sistemy [Trajectory control of observation as a way of creating intentional algorithmic effects on radar systems]. *Radiotekhnika*, 2010, no. 7. pp. 77-81 (in Russian).

352. Privalov A. A., Yevglevskaya N. V., Zubkov K. N. Model of the process for cracking the parameters pf data transmission network of IP-telephone system operator by the computer intelligence of organized intruder. *Proceedings of Petersburg Transport University*, 2014, vol. 39, no. 2, pp. 106-111 (in Russian).

353. Evglevskaya N. V., Privalov A. A., Privalov Al. A. General information impact model at the automatic systems of technical objects management. *Questions of radio-electronics*, 2013, vol. 3, no. 1, pp. 155-164 (in Russian).

354. Evglevskaya N. V., Privalov A. A., Privalov Al. A. Model of the process for opening channels of information leakage on the objectes of the telecommunications. *Questions of radio-electronics*, 2014, vol. 3, no. 1, pp. 156-161 (in Russian).

355. Evgrlevskaya N. V., Privalov A. A., Skudneva E. V. Markov model of conflict of automated information processing and management systems with the system of destructive effects of an offender. *Proceedings of Petersburg Transport University*, 2015, vol. 42, no. 1, pp. 78-84 (in Russian).

356. Evglevskaya N. V., Privalov A. A. Information impact model at the telecommunication network objects. *Proceedings of Petersburg Transport University*, 2015, vol. 42, no. 1, pp. 72-77 (in Russian).

357. Privalov A. A., Privalov Al. A., Skudneva Y. V., Chalov I. V. Approach to the assessment probabilities of breaking into space-time and information structure of data transmission's network of operational and technological use. *Proceedings of Petersburg Transport University*, 2015, vol. 44, no. 3, pp. 165-172 (in Russian).

358. Levin V. I., Nemkova E. A. Logical-Mathematical Modelling of Conflicts. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 55-64. Available at: http://sccs.intelgr.com/archive/2016-03/02-Levin.pdf (accessed 20 August 2016) (in Russian).

359. Jotsov V. S. Semantic Conflict Resolution Using Ontologies. *Proc. 2nd Intl. Conference on System Analysis and Information Technologies, SAIT*. 2007, pp. 11-14. Available at: http://195.96.242.2/staff_en/V_Jotsov/p68Caluga07.pdf (accessed 20 August 2016) (in Russian).

360. Kogalovsky M. R. Metody integratsii dannykh v informatsionnykh sistemakh [Methods of data integration in information systems]. Moscow, Institute of market problems of RAS, 2010, pp. 1-9. Available at: http://www.ipr-ras.ru/articles/kogalov10-05.pdf (accessed 20 August 2016) (in Russian).

361. Briukhov D. O., Vovchenko A. E., Zakharov V. N., Zhelenkova O. P., Kalinichenko L. A., Martynov D. O., Skvortsov N. A., Stupnikov S. A. The middleware architecture of the subject mediators for problem solving over a set of integrated heterogeneous distributed information resources in the hybrid grid-infrastructure of virtual observatories. *Informatika i ee primenenie*, 2008, vol. 2, no. 1, pp. 2-34 (in Russian).

362. Andreev A. M., Berezkin D. V., Kantonistov Iu. A. Vybor SUBD dlia postroeniia informatsionnykh sistem korporativnogo urovnia na osnove ob"ektnoi paradigmy [The choice of the DBMS for information system design corporate level on the basis of the object paradigm]. *DBMS*, 1998, no. 4-5, pp. 26-50. Available at: http://www.inteltec.ru/publish/articles/objtech/4kx4_9.shtml (accessed 25 August 2016) (in Russian).

363. Ostapenko G. A., Plotnikov D. G., Guzev Yu. N. Features of conflictology of the weighed networks: concept of the network conflict. *Informatsiia*

i bezopasnost, 2016, vol. 19, no. 1, pp. 136-137 (in Russian).

364. Ostapenko G. A., Plotnikov D. G., Guzev Yu. N. Formalization of the description of the network conflict. *Informatsiia i bezopasnost*, 2016, vol. 19, no. 2, pp. 232-237 (in Russian).

365. Ostapenko G. A., Plotnikov D. G., Guzev Yu. N. Strategy of network oppositon. *Informatsiia i bezopasnost*, 2016, vol. 19, no. 2, pp. 250-253 (in Russian).

366. Ostapenko G. A., Plotnikov D. G., Guzev Yu. N. Dinamics of development of the network conflict. *Informatsiia i bezopasnost*, 2016, vol. 19, no. 2, pp. 278-279 (in Russian).

367. Vorobev N. N. *Osnovy teorii igr. Beskoalitsionnye igry* [Fundamentals of the theory of games. Noncooperative games]. Moscow, Nauka Publ., Glavnaia redaktsiia fiziko-matematicheskoi literatury, 1984. 496 p.

368. Chudnov A. M. Teoretiko-igrovye zadachi sinteza algoritmov formirovaniia i priema signalov [Game-theoretical problems of synthesis of algorithms of formation and receiving signals]. *Problems of Information Transmission*, 1991, vol. 27, no. 3, pp. 233-240.

369. Zhodzishskii M. I. Primenenie teorii igr k sintezu optimal'noi sistemy posimvol'noi peredachi informatsii [Application of game theory to the synthesis of an optimal system character-by-character transfer of information]. *Radiotekhnika*, 1982, no. 11, pp. 77-81 (in Russian).

370. Bazar T., Wu Y. A Complete Characterization of Minimax and Maximin Encode-Decoder Policies for Communication Channels with Incomplete Statistical Description. *IEEE Transactions on Information Theory*, 1985, vol. 31, no. 4, pp. 482-489.

371. Cahn C. Performance of Digital Matched Filter Correlator with Unknown Interference. *IEEE Transactions on Information Theory*, 1971, vol. 19, no. 6, pp. 1163-1172.

372. Blackwell D. A., Girshick M. A. Theory of games and statistical decisions. – Courier Corporation, 1979.

373. Danskin J. M. *The Theory of Max-Min and Its Application to Weapons Allocation Problems*. Berlin, Springer-Verlag, 1967.

374. Neumann J., Morgenstern O. *Theory of games and economic behavior*. Princeton, Princeton university press, Vol. 60, 1944.

375. Partkhasaratkhi T., Ragkhavan T. *Nekotorye voprosy teorii igr dvukh lits* [Some questions of the theory of games of two persons]. Moscow, Mir Publ., 1974. 295 p. (in Russian).

376. Petrosian L. A., Tomskii G. V. *Dinamicheskie igry i ikh prilozheniia* [Dynamic games and their applications]. Lenigrad, Leningrad state University, 1982. 252 p. (in Russian).

377. Chernousko F. L., Melikian A. A. *Igrovye zadachi upravleniia i poiska* [Game problems of control and search]. Moscow, Nauka Publ., 1978. 270 p. (in Russian).

378. Kozlov D. G. Real'naia garantirovannaia pomekhoustoichivost' asimptoticheski optimal'nogo igrovogo priemnika psevdoshumovogo signala // [Real

guaranteed noise immunity for the asymptotically optimal gaming receiver of the pseudochromosome signal]. *Tekhnika sredstv sviazi*, 1988, no. 2, pp. 42-52 (in Russian).

379. Putilin A. N. *Radiosistemy s mnozhestvennym dostupom* [Radio systems with multiple access]. Saint-Petersburg, Military Academy of Communications, 1998. 148 p. (in Russian).

380. Putilin A. N. Model vzaimodeistviia linii radiosviazi i stantsii radioelektronnogo podavleniia [Interaction model the radio link and the station jamming]. *Trudy XIII Sankt-Peterburgskoi mezhdunarodnoi konferentsii "Regional'naia informatika (RI-2012)"* [Proceedings of the XIII Saint-Petersburg international conference "Regional Informatics (RI-2012)"]. Saint-Petersburg, Saint-Petersburg Society for computer science, computer engineering, communication systems and management, 2013. pp. 196-207 (in Russian).

381. Putilin A. N. Model funktsionirovaniia seti radiosviazi v usloviiakh radioelektronnogo podavleniia [The model of functioning of radio networks in conditions of jamming]. *Sbornik tezisov dokladov nauchnoi konferentsii "Sovremennye tendentsii razvitiia teorii i praktiki upravleniia v sistemakh spetsial'nogo naznacheniia"* [Proceedings of scientific conference "Modern trends in the theory and practice of control systems of special purpose"]. Moscow, "Sistemprom" Concern, 2013, p. 102 (in Russian).

382. Yuditskiy S. A. Modelirovanie dinamiki mnogoagentnykh triadnykh setei [Simulation of the dynamics Multi-agent of networks]. Moscow, SINTEG Publ., 2012. 112 p. (in Russian).

Статья поступила 1 августа 2016 г.
Доработана и принята к публикации 16 сентября 2016 г.

Информация об авторах

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.

Михайлов Роман Леонидович – кандидат технических наук. Старший научный сотрудник. Череповецкое высшее военное инженерное училище радиоэлектроники. Область научных интересов: устойчивость сетей связи, маршрутизация информационных потоков, комплексное воздействие на сети связи средств наблюдения и подавления. E-mail: mikhailov-rom2012@yandex.ru

Адрес: 162622, Вологодская обл., г. Череповец, Советский пр., д. 126.

Information Conflicts – Analysis of Papers and Research Methodology

S. I. Makarenko, R. L. Mikhailov

Relevance. *Now the methodology of the theory of information warfare in the technical field is formed as the development and joining of theories of electronic warfare and information security. The development of the theory of information warfare is strongly associated with the theory of conflict, in particular with the theory of information conflict. Therefore, the analysis of famous papers and research methodology of the information conflict is relevant.* ***The aim of this paper*** *is the analysis of the known researches of the information conflict. Special attention is paid to the analysis of the conflict between a communication system, a radio monitoring system and an electronic warfare system.* ***Methods used.*** *Analysis of the theory of the informational conflict is based on the use of the methods of system analysis, the methods of induction and deduction of the logic theory.* ***Result.*** *General and specific patterns of research the information conflict was identified based on the analysis of more than 300 references. The analysis of the patterns of the information conflict was based on the researches that were conducted using different scientific methodological apparatus. The theory of active systems, the dynamical systems theory, the game theory, the theory of Markov processes, the theory of Petri nets, the theory of complex hierarchical systems, and other theories relates to the scientific-methodical apparatus, which were considered. The paper proves that new and interesting ways of research for the information conflict is the consideration factors of complexity and multilevel of conflicting systems, the multistage character of the flow of the conflict; the consideration of hidden influences in the process of the conflict, as well as the dynamic properties of the conflict. These factors can be taken into account if the information conflict will be formalized based on the theory of dynamical systems, the bifurcation theory, the catastrophe theory and the deterministic chaos theory.* ***Novelty.*** *The element of novelty of this paper is general and specific patterns, the approaches to the study of information conflict which were identified in the analysis of famous papers. Also the elements of novelty are specific trends research for the information conflicts between the communications system, the radio monitoring system and the jamming system.* ***Practical significance.*** *The analysis presented in this paper can be used by technical specialists to justify new technological solutions for the electronic warfare systems, the information warfare systems, the radio monitoring systems and the communication systems. This analysis can be used military specialists to support new forms and methods of armed acts too. In addition, this analysis will be useful to scientists conducting researches in the field of the information conflict.*

Key words: *conflict, information conflict, communication systems, electronic warfare, radiomonitoring, information struggle.*

Information about Authors

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. A. F. 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, Zjdanovskaya ulica, 13.

Roman Leonidovich Mikhailov – Ph.D. of Engineering Sciences. Senior Researcher. Cherepovets Higher Military Engineering School of Radio Electronics. Field of research: sustainability of communication, routing of data flow, unified influence of monitoring and rejection means on communication networks. E-mail: mikhailov-rom2012@yandex.ru

Address: Russia, 162622, Vologda region, Cherepovets, Sovetskiy prospect, 126.

УДК 681.3.06 (075.32)

Инновации: от устройств обмена информацией до интегрированных систем управления

Часть 2 – Управление деятельностью организационных систем

Шабанов А. П.

Введение: *рассматриваются изобретения, которые относятся к критическим технологиям – технологиям информационных и управляющих систем, определяющих, наряду с другими, основные направления научно-технического развития.* ***Характеристика:*** *разработка представленных технических решений осуществлялась в двух временных интервалах новейшей истории отечественной электронной промышленности – во время становления интеграционных научно-производственных комплексов и постановки масштабных системных проектов в 1980-е годы, и во время восстановления этого подхода в 2010-е годы. В первом периоде были разработаны технические решения по сбору и обработке актуальной информации об объектах управления, по повышению устойчивости функционирования трактов компьютерных сетей с использованием средств радиосвязи и оптоволоконной связи, по управлению временем предоставления информации. Во втором периоде эти технические решения послужили основой для разработки инновационных способов информационной поддержки деятельности организационных систем – ведомств, предприятий, учреждений, и разработки интегрированных систем управления для организационных систем, выполняющих общие задачи.* ***Технический результат.*** *Использование технических решений, разработанных в первом периоде, повышает качественные показатели управления и связи по своевременности и надежности предоставления информации. Использование технических решений, разработанных во втором периоде, позволяет обеспечить максимальную степень автоматизации процессов управления на основе подготовки априорных сценариев для принятия и исполнения управляющих решений.* ***Суть:*** *общее, что объединяет изобретения обоих периодов, является авторский подход, который был применен к поиску идеи изобретения и к его структурному воплощению. Данный подход включает в себя, помимо общеприменяемых, этапы формирования, накопления и использования знаний о сущностях, которые влияют на область деятельности, рассматриваемую в процессах функционирования разрабатываемых способов, систем и устройств. При этом использование этих знаний осуществляется путем обработки данных в компонентах вычислительных комплексов и компьютерных сетей с воздействием на порядок расположения данных и на их содержание.* ***Практическая значимость:*** *информация об изобретениях, разработанных в первом периоде, была опубликована в предыдущем выпуске журнала с целью возможного использования идей, лежащих в их основе, для воплощения на базе современных средств вычислительной техники. Информация об изобретениях, разработанных во втором периоде и относящаяся к управлению деятельностью организационных систем, приводится в этой статье с целью расширения потенциальной области их внедрения в практику управления организационными системами. Это позволит непрерывно отслеживать состояние деятельности и сократить время на принятие и исполнение управляющих решений в ведомствах, на предприятиях и в учреждениях.*

Ключевые слова*: изобретения, критические технологии, системы управления, информационные системы, системы связи, накопление знаний, сценарии решений.*

Постановка задачи

Государственная политика, проводимая в настоящее время в сфере обеспечения национальной безопасности и социально-экономического развития Российской Федерации на фоне новых угроз, имеющих комплексный взаимосвязанный характер, требует устранения структурных дисбалансов в экономике и ее модернизации, повышения обороноспособности страны.

Обеспечение национальных интересов должно осуществляться посредством реализации стратегических национальных приоритетов, в том числе [1]:

- совершенствование научно-технической поддержки правоохранительной деятельности;
- повышение эффективности пограничной деятельности, включая совершенствование межведомственного взаимодействия и межгосударственного пограничного сотрудничества;
- развитие единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, ее территориальных и функциональных подсистем, взаимодействия с аналогичными иностранными системами;
- развитие информационной инфраструктуры с возможностью получения равного доступа к государственным услугам на всей территории Российской Федерации, в том числе с использованием информационных и коммуникационных технологий;
- обеспечение экономической безопасности, включая развитие промышленно-технологической базы и национальной инновационной системы, модернизацию и развитие приоритетных секторов национальной экономики;
- осуществление рационального импортозамещения, снижение критической зависимости от зарубежных технологий и промышленной продукции;
- завершение формирования базовой информационной инфраструктуры и других.

Представляется очевидным, что реализацию стратегических национальных приоритетов осуществить без создания перспективных информационных технологий затруднительно. При этом, как показывает анализ приведенного выше списка приоритетов, одной из наиболее важных задач развития информационных технологий является совершенствование и разработка новых способов и систем управления деятельностью организационных систем в ведомствах и органах управления различного уровня, на предприятиях и в учреждениях.

Задачей настоящей статьи является представление инновационных технических решений – изобретений и полезных моделей, которые относятся к критическим технологиям – технологиям информационных и управляющих систем [2]. Эти технологии, наряду с другими, определяют основные направления научно-технического развития.

Разработка представленных в настоящей статье технических решений осуществлялась в новейшей истории отечественной электронной промышленности – в 2010-е годы. Представленные решения развивают идеи, заложенные в разработках, выполненных с участием автора во время становления интеграционных научно-производственных комплексов и постановки масштабных системных проектов в 1980-е годы. В том периоде были разработаны технические решения по сбору и обработке актуальной

информации об объектах управления, по повышению устойчивости функционирования трактов компьютерных сетей с использованием средств радиосвязи и оптоволоконной связи, по управлению временем предоставления информации и другие [3].

Представленные в настоящей статье технические решения относятся к инновационным системам управления деятельностью организационных систем и способам поддержки их деятельности – деятельности ведомств, предприятий, учреждений, органов власти и их подразделений. Использование данных изобретений и полезных моделей позволяет обеспечить максимальную степень автоматизации процессов управления на основе подготовки и применения априорных и ретроспективных сценариев для автоматического их исполнения робототехническими объектами, информационными системами или для принятия решений субъектами управления в зависимости от имеющихся ресурсов и сложившихся обстоятельств в среде деятельности.

Общее, что объединяет изобретения обоих периодов, является авторский подход, который был применен к поиску идей инновационных решений и к их структурному представлению. Данный подход включает в себя, помимо обще применяемых, этапы формирования, накопления и использования знаний о сущностях, которые влияют на виды деятельности, рассматриваемые в процессах функционирования разрабатываемых способов, систем и центров. Использование этих знаний осуществляется путем введения в составные части технических решений – в вычислительные комплексы и компьютерные сети, механизмов обработки данных с воздействием на порядок расположения данных и на их содержание.

Информация об изобретениях и полезных моделях, представленных в настоящей статье, приводится с целью расширения потенциальной области их внедрения в отечественную практику управления деятельностью организационных систем. Это позволит непрерывно отслеживать состояние предметной области деятельности и сократить время на принятие и исполнение управляющих решений.

Система управления деятельностью организационных систем

Характеристика области управления. Техническое решение «Система управления деятельностью организационных систем» [4] относится к области управления деятельностью организационных систем. Предметной областью являются системы управления объектами наблюдения в контролируемом пространстве и во внешней среде, включая информационные системы и сети, робототехнические объекты, которые оказывают влияние на состояние деятельности организационных систем.

Системы управления деятельностью организационных систем являются концентрацией современных информационных технологий, предназначенных для автоматизированного и автоматического управления деятельностью организационных систем – государственных служб, предприятий и учреждений, для автоматического управления технологическими системами, для управления робототехническими объектами. В настоящее время широкое

применение находят системы управления двойного и многофункционального назначения. Это системы, которые обеспечивают управление различными видами деятельности организационных систем, принципиально отличающимися между собой. Системы управления собирают данные о фактических показателях объектов наблюдения, производят на основе этих данных анализ эффективности деятельности. На основе результатов анализа и априорно записанных данных об информационных моделях сценариев управления производят управляющие воздействия на объекты наблюдения в контролируемом пространстве и во внешней среде, включая информационные системы и сети, робототехнические объекты, которые оказывают влияние на деятельность организационных систем. Тем самым, обеспечивают управление деятельностью организационных систем. Примерами систем управления двойного назначения являются: центр объективного контроля [5], система управления воздушным движением объектов гражданского и военного назначения [6]. Указанные выше системы управления являются аналогами настоящего технического решения.

Преимуществом системы управления деятельностью организационных систем [4], по сравнению с её аналогами, является *обеспечение возможности* автоматической проверки актуальности данных о выбранном для исполнения сценарии управления, переформировании, при необходимости, этих данных, запоминании и передачи их для управления робототехническими объектами и объектами наблюдения, оказывающими влияние на деятельность организационных систем с учётом выполненной проверки. Так, например, несмотря на периодически проводимые организационные мероприятия – аудиты, не исключаются ситуации, при которых выбранный сценарий управления не может быть выполнен по причине произведённых в интервале времени между периодическими аудитами изменениях в силах и/или средствах организационных систем, данные о которых не актуализированы в их информационных моделях. К таким изменениям относятся: установка новых или обновление существующих версий программ; установка новых или перенастройка существующих аппаратных средств; изменение штатного расписания и другие изменения. В результате вышеизложенного, время перерывов в деятельности организационных систем, обусловленных значительным числом проблемных или угрожающих ситуаций, может быть увеличено за счёт времени на поиск причин невыполнения работ в соответствии с принятым для управления сценарием, но данные о котором являются не достоверными.

При разработке технического решения [4] использовалась следующая логически взаимосвязанная цепь суждений:

1) чем менее продолжительны перерывы в деятельности организационной системы, обусловленные возможными негативными ситуациями и угрозами, тем выше эффективность системы управления;
2) чем выше степень автоматизации системы управления, определяемая, в том числе, наличием и достоверностью информационных моделей – данных о сценариях управления, тем меньше осуществлённых угроз и

менее продолжительны перерывы в деятельности организационных систем;

3) технические решения, которые обеспечивают целевой аудит и поддержание в актуальном состоянии данных о сценариях управления, тем самым обеспечивают повышение достоверности этих данных, повышение эффективности системы управления и, в целом, повышение эффективности деятельности организационных систем.

Задачей, на решение которой направлено данное техническое решение, является предложение новой и улучшенной системы управления деятельностью организационных систем, способной сократить сроки разрешения проблемных ситуаций, предотвращения угроз и повышения эффективности выполнения плановых работ.

Технический результат заключается в автоматической проверке актуальности данных о выбранном для исполнения сценарии управления, при необходимости переформировании этих данных, запоминании и использовании их для управления робототехническими объектами и другими объектами наблюдения, оказывающими влияние на состояние деятельности организационных систем, с учётом выполненной проверки. Технический результат достигается, прежде всего, проведением целевого аудита (проверки актуальности) данных о выбранном сценарии управления до момента передачи этих данных для исполнения в информационные сети организационных систем и/или их подразделений и/или для управления робототехническими объектами.

Описание технического решения. Структурная схема системы управления деятельностью организационных систем представлена на рис. 1.

Система обеспечивает управление деятельностью организационных систем и их подразделений. Для передачи данных между системой управления и информационными сетями организационных систем и их подразделений используется телекоммуникационная сеть. Система управления деятельностью организационных систем содержит:

- аналитический центр, содержащий вычислительный комплекс, систему хранения данных аудита деятельности организационных систем (далее по тексту, система хранения данных), комплекс средств аудита и комплекс средств моделирования;
- центр объективного контроля, содержащий компьютерную сеть, мультимедиа – проектор с экраном, видеосистему и компьютер настройки видеосистемы;
- информационную сеть;
- преобразователь данных;
- средства контроля в объектах наблюдения в контролируемом пространстве и/или вне объектов наблюдения, с возможностью наблюдения над ними;
- средства двухсторонней проводной и/или беспроводной связи (далее по тексту, средства связи – для связи средств контроля с информационной сетью);
- средства связи и средства кодирования в робототехнических объектах.

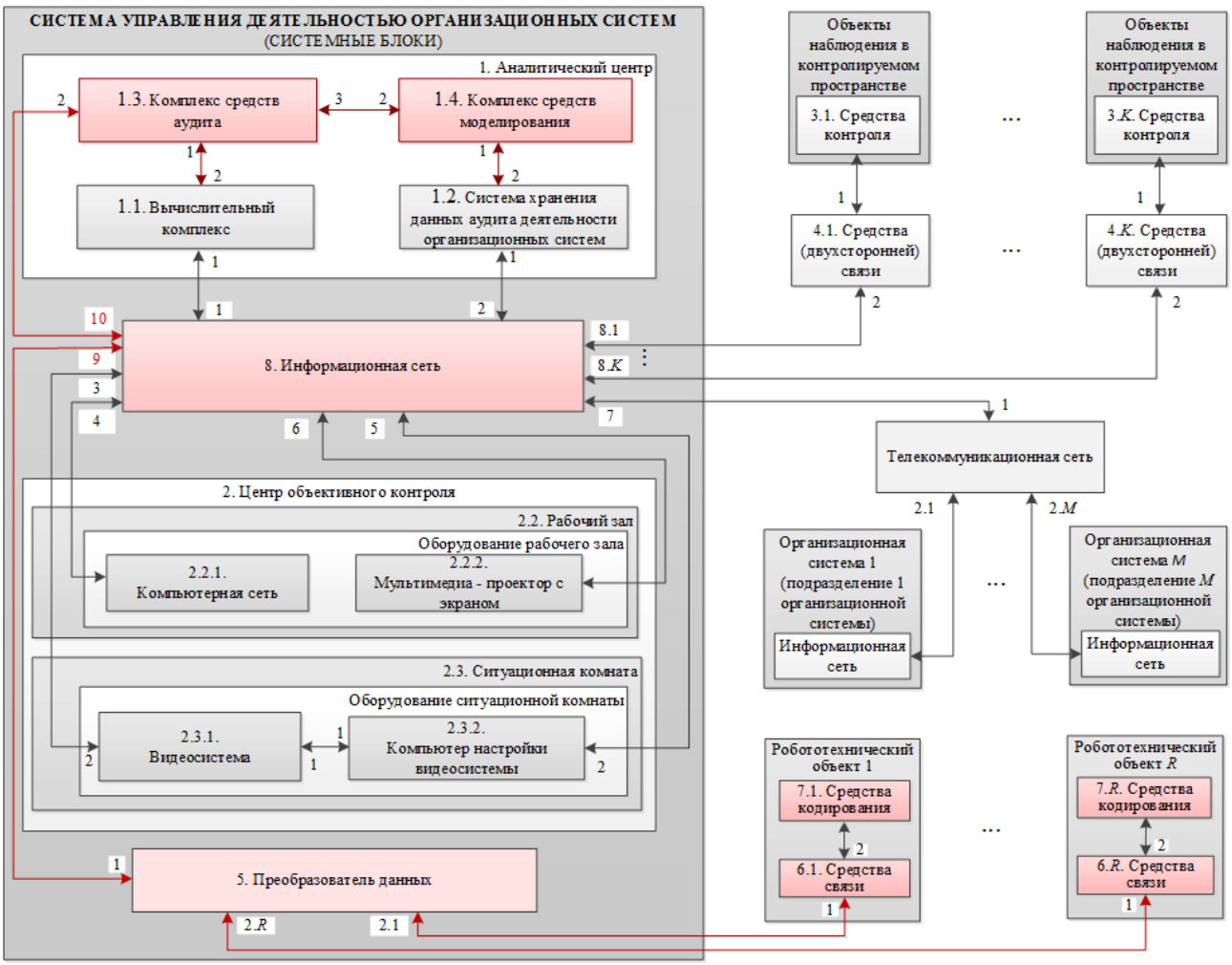


Рис. 1. Структурная схема системы управления деятельностью организационных систем

Средства контроля включают: блок формирования телеметрической цифровой информации, и/или блок указания координат объекта наблюдения, и/или контролируемого участка объекта наблюдения, блок указания фактического времени контроля над состоянием объекта наблюдения, блок создания видеоизображения объекта наблюдения, блоки формирования данных о показателях наблюдаемых объектов, представленных безразмерными числами и/или единицами измерений.

Средства связи для объектов наблюдения соединены, с одной стороны, с информационной сетью, с другой стороны, со средствами контроля над объектами наблюдения. Объекты наблюдения представляют собой такие субъекты, материальные и нематериальные объекты в организационных системах и во внешней среде, которые оказывают влияние на состояние деятельности организационных систем и на состояние робототехнических объектов.

Средства связи робототехнических объектов соединены, с одной стороны, с преобразователем данных, с другой стороны, со средствами кодирования в робототехнических объектах. Робототехнические объекты – это роботы и автоматические системы, предназначенные для управления объектами наблюдения и другими объектами в соответствии:

– с записанными в робототехнических объектах и в управляемых ими объектах программами;
– с данными о сценариях управления, включая данные о командах управления, поступающими в средства кодирования робототехнических объектов из преобразователя данных.

Система управления деятельностью организационных систем соединена посредством информационной сети и единой для организационных систем телекоммуникационной сети с информационными сетями организационных систем (подразделений организационных систем). Образованные таким образом тракты передачи данных предназначены для передачи в автоматическом режиме данных о сценариях управления:

– в объекты наблюдения и другие объекты, которые подключены к информационным сетям организационных систем (их подразделений) для непосредственного производства управляющих воздействий в автоматическом режиме в соответствии с записанными в этих объектах программами и данными о сценариях управления (адресные данные объектов и их управляющих и управляемых элементов, данные о командах, другие данные);
– в персональные компьютеры или рабочие станции исполнителей сценариев управления, с целью производства управляющих воздействий над объектами наблюдения и другими объектами в автоматизированном режиме в соответствии с данными о сценариях управления.

Система управления деятельностью организационных систем выполнена таким образом, что в ней формируются, сохраняются и отображаются на экранах видеосистем следующие технологические данные:

– данные D о требуемом состояния деятельности всех организационных систем в целом (далее по тексту, деятельности консолидированной организационной системы);
– данные D_n о требуемом состоянии n-го вида деятельности консолидированной организационной системы, n=1, 2, …, N;
– данные α_n о назначенном приоритете для n-го вида деятельности консолидированной организационной системы;
– данные S_{nm} о требуемом состоянии n-го вида деятельности, осуществляемой в m-ой организационной системе, m=1, 2, …, M;
– данные β_{nm} о приоритете n-го вида деятельности, осуществляемой в m-ой организационной системе;
– данные S_{nm}, которые формируются следующим образом: $S_{nm} = \gamma_{nm1}V_{nm1} + \gamma_{nm2}V_{nm2} + \ldots + \gamma_{nmK}V_{nmK}$;
– V_{nmk} – данные о требуемом состоянии k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе, k=1, 2, …, K;
– данные γ_{nmk} о приоритете k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой

организационной системе;

- данные V^l_k о требуемом l-ом показателе состояния k-го объекта наблюдения, l=1, 2, …, $L(k)$, где $L(k)$ – число показателей, которые применяются для характеристики состояния k-го объекта наблюдения;
- данные V^l_k представляются безразмерными числами, временными, метрическими, весовыми, стоимостными и другими единицами измерений; в состав данных о требуемых показателях объекта наблюдения входят данные о требуемых показателях физических, логических, информационных, территориальных, конструктивных, организационных и других типов связи k-го объекта наблюдения с другими объектами наблюдения;
- данные μ^l_k о приоритете l-ого показателя состояния k-го объекта наблюдения;
- данные V^l_{nmk} о требуемом l-ом показателе состояния k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе;
- данные V^l_{nmk} формируются следующим образом:
  - $V^l_{nmk}=V^l_k$, если k-ый объект наблюдения оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе;
  - $V^l_{nmk}=0$ – в противном случае;
- данные V_{nmk} формируются следующим образом: $V_{nmk} = \mu^1_k V^1_{nmk} + \mu^2_k V^2_{nmk} + \ldots + \mu^{L(k)}_k V^{L(k)}_{nmk}$.

Система управления деятельностью организационных систем выполнена таким образом, что в ней с помощью средств контроля производится измерение показателей объектов наблюдения, их преобразование в цифровой вид и формирование данных V^{*l}_{nmk} о фактическом l показателе k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе, где l=1, 2,…, $L(k)$; k=1, 2, …, K; n=1, 2, …, N; m=1, 2, …, M. Данные V^{*l}_{nmk} представляются безразмерными числами, временными, метрическими, весовыми, стоимостными и другими единицами измерений. После формирования и сохранения данных V^{*l}_{nmk} формируются, сохраняются и отображаются на экранах следующие данные:

- данные ΔV^{*l}_{nmk} об абсолютном значении отклонения данных V^{*l}_{nmk}, о фактическом l показателе k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе, от данных V^l_{nmk} о требуемом l показателе k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе: $\Delta V^{*l}_{nmk} = |V^l_{nmk} - V^{*l}_{nmk}|$;
- данные V^*_{nmk} о фактическом состоянии k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе, при этом

$V^*_{nmk} = \mu^1_k (V^1_{nmk} - \Delta V^{*1}_{nmk}) + \mu^2_k (V^2_{nmk} - \Delta V^{*2}_{nmk}) + \ldots + \mu^{L(k)}_k (V^{*L(k)}_{nmk} - V^{*L(k)}_{nmk})$;

- данные S^*_{nm} о фактическом состоянии n-го вида деятельности, осуществляемой в m-ой организационной системе, при этом $S^*_{nm} = \gamma_{nm1} V^*_{nm1} + \gamma_{nm2} V^*_{nm2} + \ldots + \gamma_{nmK} V^*_{nmK}$;
- данные ΔS^*_{nm} о фактическом показателе эффективности n-го вида деятельности в m-ой организационной системе, при этом $\Delta S^*_{nm} = S^*_{nm} / S_{nm}$;
- данные $\Delta S_{nm\text{-крит.}}$ о показателе эффективности n-го вида деятельности, осуществляемой в m-ой организационной системе, снижение, по сравнению с которым, фактического показателя означает существование угрозы для n-го вида деятельности в m-ой организационной системе и необходимости принятия действий по её устранению;
- данные $\Delta S_{nm\text{-доп.}}$ о показателе эффективности n-го вида деятельности, осуществляемой в m-ой организационной системе, снижение, по сравнению с которым, фактического показателя означает возможность появления угрозы для n-го вида деятельности в m-ой организационной системе и необходимости принятия действий по предупреждению появления угрозы.
- данные D_n о требуемом состоянии n-го вида деятельности консолидированной организационной системы, при этом $D_n = \beta_{n1} S_{n1} + \beta_{n2} S_{n2} + \ldots + \beta_{nM} S_{nM}$;
- данные D^*_n о фактическом состоянии n-го вида деятельности консолидированной организационной системы, при этом $D^*_n = \beta_{n1} S^*_{n1} + \beta_{n2} S^*_{n2} + \ldots + \beta_{nM} S^*_{nM}$;
- данные ΔD^*_n о фактическом показателе эффективности n-го вида деятельности консолидированной организационной системы, при этом $\Delta D^*_n = D^*_n / D_n$;
- данные $\Delta D_{n\text{-крит.}}$ о критическом показателе эффективности n-го вида деятельности консолидированной организационной системы, снижение, по сравнению с которым, фактического показателя означает существование угрозы для этого вида деятельности консолидированной организационной системы и необходимости принятия действий по её устранению;
- данные $\Delta D_{n\text{-доп.}}$ о допустимом показателе эффективности n-го вида деятельности консолидированной организационной системы, снижение, по сравнению с которым, фактического показателя означает возможность появления угрозы для этого вида деятельности консолидированной организационной системы и необходимости принятия действий по предупреждению появления угрозы;
- данные D о требуемом состоянии деятельности консолидированной организационной системы в целом, при этом $D = \alpha_1 D_1 + \alpha_2 D_2 + \ldots + \alpha_N D_N$;

– данные D^* о фактическом состоянии деятельности консолидированной организационной системы в целом, при этом $D^* = \alpha_1 D^*_1 + \alpha_2 D^*_2 + \ldots + \alpha_N D^*_N$;
– данные ΔD^* о фактическом показателе эффективности деятельности консолидированной организационной системы в целом, при этом $\Delta D^* = D^*/D$;
– данные $\Delta D_{крит.}$ о критическом показателе эффективности деятельности консолидированной организационной системы в целом, снижение, по сравнению с которым, фактического показателя ΔD^* эффективности деятельности консолидированной организационной системы в целом означает существование угрозы для деятельности консолидированной организационной системы в целом и необходимости принятия действий по её устранению;
– данные $\Delta D_{доп.}$ о допустимом показателе эффективности деятельности консолидированной организационной системы в целом, снижение, по сравнению с которым, фактического показателя ΔD^* эффективности деятельности консолидированной организационной системы в целом означает возможность появления угрозы для деятельности консолидированной организационной системы в целом и необходимости принятия действий по предупреждению появления угрозы.

Система управления деятельностью организационных систем выполнена таким образом, что в ней формируются, сохраняются и отображаются на экранах следующие данные о сценариях управления (далее по тексту, сценариях):

– данные $Q_{крит.}$ о числе критических сценариев, предназначенных для управления ликвидацией угрозы для деятельности консолидированной организационной системы в целом;
– данные $W_{крит.}$ о множестве критических сценариев, предназначенных для управления ликвидацией угрозы для деятельности консолидированной организационной системы в целом при условии $0 \le \Delta D^* < \Delta D_{крит.}$, при этом

$W_{крит.} = \{W^1_{крит.}$ или $W^2_{крит.}$ … или $W^{Q крит.}_{крит.}\}$, где

$W^{q1}_{крит.}$ – данные о $q1$-ом критическом сценарии, предназначенном для управления ликвидацией угрозы для деятельности консолидированной организационной системы в целом,

$q1$ – данные о приоритете критического сценария,

$q1 = 1, 2, \ldots, Q_{крит.}$, при этом выполняется условие

$$P(W^{q1}_{крит.}) \ge P(W^{q1-1}_{крит.}),\ \sum_{q1=1}^{Q_{крит.}} P(W^{q1}_{крит}) = 1, \text{ где}$$

$P(W^{q1}_{крит.})$ и $P(W^{q1-1}_{крит.})$ – соответственно данные о прогнозируемых вероятностях для выбора критического сценария $W^{q1}_{крит.}$ и критического сценария $W^{q1-1}_{крит.}$, $P(W^0_{крит.}) = 0$;

– данные $Q_{пред.}$ о числе предупреждающих сценариев, предназначенных

для управления предотвращением угрозы для деятельности консолидированной организационной системы в целом;

– данные $W_{\text{пред.}}$ о множестве предупреждающих сценариев, предназначенных для управления предотвращением угрозы для деятельности консолидированной организационной системы в целом при условии $\Delta D_{\text{крит.}} \leq \Delta D^* < \Delta D_{\text{доп.}}$, при этом

$W_{\text{пред.}} = \{W^1{}_{\text{пред.}}$ или $W^2{}_{\text{пред.}}$ … или $W^{Q\text{пред.}}{}_{\text{пред.}}\}$, где

$W^{q2}{}_{\text{пред.}}$ – данные о $q2$-ом предупреждающем сценарии,

$q2$ – данные о приоритете этого сценария,

$q2 = 1, 2, \ldots, Q_{\text{пред.}}$, при этом выполняется условие

$P(W^{q2}{}_{\text{пред.}}) \geq P(W^{q2\text{-}1}{}_{\text{пред.}})$, $\sum_{q2=1}^{Q_{пред.}} P(W^{q2}_{пред}) = 1$, где

$P(W^{q2}{}_{\text{пред.}})$ и $P(W^{q2\text{-}1}{}_{\text{пред.}})$ – соответственно данные о прогнозируемых вероятностях для выбора предупреждающего сценария $W^{q2}{}_{\text{пред.}}$ и предупреждающего сценария $W^{q2\text{-}1}{}_{\text{пред.}}$, $P(W^0{}_{\text{пред.}}) = 0$;

– данные $Q_{\text{план.}}$ о числе плановых сценариев, предназначенных для управления плановой деятельностью консолидированной организационной системы в целом;

– данные $W_{\text{план.}}$ о множестве плановых сценариев, предназначенных для управления плановой деятельностью консолидированной организационной системы в целом при условии $\Delta D_{\text{доп.}} \leq \Delta D^* < 1$, при этом $W_{\text{план.}} = \{W^1{}_{\text{план.}}$ или $W^2{}_{\text{план.}}$ … или $W^{Q\text{план.}}{}_{\text{план.}}\}$, где

$W^{q3}{}_{\text{план.}}$ – данные о $q3$-ом плановом сценарии,

$q3$ – данные о приоритете этого сценария,

$q3 = 1, 2, \ldots, Q_{\text{план.}}$, при этом выполняется условие

$P(W^{q3}{}_{\text{план.}}) \geq P(W^{q3\text{-}1}{}_{\text{план.}})$, $\sum_{q3=1}^{Q_{план.}} P(W^{q3}_{план.}) = 1$, где

$P(W^{q3}{}_{\text{план.}})$ и $P(W^{q3\text{-}1}{}_{\text{план.}})$ – соответственно данные о прогнозируемых вероятностях для выбора планового сценария $W^{q3}{}_{\text{план.}}$ и планового сценария $W^{q3\text{-}1}{}_{\text{план.}}$, $P(W^0{}_{\text{план.}}) = 0$;

– данные $U_{n\text{-крит.}}$ о числе критических сценариях, предназначенных для управления ликвидацией угрозы для n-го вида деятельности консолидированной организационной системы;

– данные $W^n{}_{\text{крит.}}$ о множестве критических сценариев, предназначенных для управления ликвидацией угрозы для n-го вида деятельности консолидированной организационной системы при условии $0 \leq \Delta D^*_n < \Delta D_{n\text{-крит.}}$, при этом

$W^n{}_{\text{крит.}} = \{W^{n1}{}_{\text{крит.}}$ или $W^{n2}{}_{\text{крит.}}$ … или $W^{nUn\text{-крит.}}{}_{\text{крит.}}\}$, где

$W^{nu1}{}_{\text{крит.}}$ – данные об $u1$-ом критическом сценарии, предназначенном для управления ликвидацией угрозы для n-го вида деятельности консолидированной организационной системы,

$u1$ – данные о приоритете критического сценария,

$u1 = 1, 2, \ldots, U_{n\text{-крит.}}$, при этом выполняется условие

$P(W^{nu1}_{\text{крит.}}) \geq P(W^{n(u1-1)}_{\text{крит.}})$, $\sum_{u1=1}^{U_{n-крит.}} P(W^{nu1}_{крит.}) = 1$, где

$P(W^{nu1}_{\text{крит.}})$ и $P(W^{n(u1-1)}_{\text{крит.}})$ – соответственно данные о прогнозируемых вероятностях для выбора критического сценария $W^{nu1}_{\text{крит.}}$ и критического сценария $W^{n(u1-1)}_{\text{крит.}}$, $P(W^{n0}_{\text{крит.}})=0$;

– данные $U_{n\text{-пред.}}$ о числе предупреждающих сценариях, предназначенных для управления предотвращением угрозы для n-го вида деятельности консолидированной организационной системы;

– данные $W^{n}_{\text{пред.}}$ о множестве предупреждающих сценариев, предназначенных для управления предотвращением угрозы для n-го вида деятельности консолидированной организационной системы при условии $\Delta D_{n\text{-крит.}} \leq \Delta D^*_n < \Delta D_{n\text{-доп.}}$, при этом

$W^{n}_{\text{пред.}} = \{W^{n1}_{\text{пред.}}$ или $W^{n2}_{\text{пред.}} \ldots$ или $W^{nUn\text{-пред.}}_{\text{пред.}}\}$, где

$W^{nu2}_{\text{пред.}}$ – данные об $u2$-ом предупреждающем сценарии, предназначенном для управления предотвращением угрозы для n-го вида деятельности консолидированной организационной системы,

$u2$ – данные о приоритете предупреждающего сценария,

$u2 = 1, 2, \ldots, U_{n\text{-пред.}}$, при этом выполняется условие

$P(W^{nu2}_{\text{пред.}}) \geq P(W^{n(u2-1)}_{\text{пред.}})$, $\sum_{u2=1}^{U_{n-пред.}} P(W^{nu2}_{пред.}) = 1$, где

$P(W^{nu2}_{\text{пред.}})$ и $P(W^{n(u2-1)}_{\text{пред.}})$ – соответственно данные о прогнозируемых вероятностях для выбора предупреждающего сценария $W^{nu2}_{\text{пред.}}$ и предупреждающего сценария $W^{n(u2-1)}_{\text{пред.}}$, $P(W^{n0}_{\text{пред.}})=0$;

– данные $U_{n\text{-план.}}$ о числе плановых сценариях, предназначенных для управления плановой n-го вида деятельностью консолидированной организационной системы;

– данные $W^{n}_{\text{план.}}$ о множестве плановых сценариев, предназначенных для управления плановой n-го вида деятельностью консолидированной организационной системы при условии $\Delta D_{n\text{-доп.}} \leq \Delta D^*_n < 1$, при этом

$W^{n}_{\text{план.}} = \{W^{n1}_{\text{план.}}$ или $W^{n2}_{\text{план.}} \ldots$ или $W^{nUn\text{-план.}}_{\text{план.}}\}$, где

$W^{nu3}_{\text{план.}}$ – данные о $u3$-ом плановом сценарии, предназначенном для управления плановой n-го вида деятельностью консолидированной организационной системы,

$u3$ – данные о приоритете планового сценария,

$u3 = 1, 2, \ldots, U_{n\text{-план.}}$, при этом выполняется условие

$P(W^{nu3}_{\text{план.}}) \geq P(W^{n(u3-1)}_{\text{план.}})$, $\sum_{u3=1}^{U_{n-план.}} P(W^{nu3}_{план.}) = 1$, где

$P(W^{nu3}_{\text{план.}})$ и $P(W^{n(u3-1)}_{\text{план.}})$ – соответственно данные о прогнозируемых вероятностях для выбора предупреждающего сценария $W^{nu3}_{\text{план.}}$ и предупреждающего сценария $W^{n(u3-1)}_{\text{план.}}$, $P(W^{n0}_{\text{план.}})=0$;

– данные $Y_{nm\text{-крит.}}$ о числе критических сценариев, предназначенных для управления ликвидацией угрозы для n-го вида деятельности в m-ой организационной системе;

– данные $W^{nm}_{\text{крит.}}$ о множестве критических сценариев, предназначенных

для управления ликвидацией угрозы для n-го вида деятельности в m-ой организационной системе при условии $0 \le \Delta S^*_{nm} < \Delta S_{nm\text{-крит.}}$, при этом $W^{nm}{}_{\text{крит.}} = \{W^{nm1}{}_{\text{крит.}}$ или $W^{nm2}{}_{\text{крит.}} \ldots$ или $W^{nmYnm\text{-крит.}}{}_{\text{крит.}}\}$, где

$W^{nmy1}{}_{\text{крит.}}$ – данные о $y1$-ом критическом сценарии, предназначенном для управления ликвидацией угрозы для n-го вида деятельности в m-ой организационной системе,

$y1$ – данные о приоритете критического сценария;

$y1 = 1, 2, \ldots, Y_{nm\text{-крит.}}$, при этом выполняется условие

$P(W^{nmy1}{}_{\text{крит.}}) \ge P(W^{nm(y1-1)}{}_{\text{крит.}})$, $\sum_{y1=1}^{Y_{nm-крит.}} P(W_{крит}^{nmy1}) = 1$, где

$P(W^{nmy1}{}_{\text{крит.}})$ и $P(W^{nm(y1-1)}{}_{\text{крит.}})$ – соответственно данные о прогнозируемых вероятностях для выбора критического сценария $W^{nmy1}{}_{\text{крит.}}$ и критического сценария $W^{nm(y1-1)}{}_{\text{крит.}}$, $P(W^{nm0}{}_{\text{крит.}})=0$;

– данные $Y_{nm\text{-пред.}}$ о числе предупреждающих сценариев, предназначенных для управления предотвращением угрозы для n-го вида деятельности в m-ой организационной системе;

– данные $W^{nm}{}_{\text{пред.}}$ о множестве предупреждающих сценариев, предназначенных для управления предотвращением угрозы для n-го вида деятельности в m-ой организационной системе при условии $\Delta S_{nm\text{-крит.}} \le \Delta S^*_{nm} < \Delta S_{nm\text{-доп.}}$, при этом

$W^{nm}{}_{\text{пред.}} = \{W^{nm1}{}_{\text{крит.}}$ или $W^{nm2}{}_{\text{крит.}} \ldots$ или $W^{nmYnm\text{-крит.}}{}_{\text{крит.}}\}$, где

$W^{nmy2}{}_{\text{пред.}}$ – данные о $y2$-ом предупреждающем сценарии, предназначенном для управления предотвращением угрозы для n-го вида деятельности в m-ой организационной системе,

$y2$ – данные о приоритете предупреждающего сценария;

$y2 = 1, 2, \ldots, Y_{nm\text{-пред.}}$, при этом выполняется условие

$P(W^{nmy2}{}_{\text{пред.}}) \ge P(\mathrm{W}^{nm(y2-1)}{}_{\text{пред.}})$, $\sum_{y2=1}^{Y_{nm-пред.}} P(W_{пред}^{nmy2}) = 1$, где

$P(W^{nmy2}{}_{\text{пред.}})$ и $P(W^{nm(y2-1)}{}_{\text{пред.}})$ – соответственно данные о прогнозируемых вероятностях для выбора предупреждающего сценария $W^{nmy2}{}_{\text{пред.}}$ и предупреждающего сценария $W^{nm(y2-1)}{}_{\text{пред.}}$, $P(W^{nm0}{}_{\text{пред.}})=0$;

– данные $Y_{nm\text{-план.}}$ о числе плановых сценариях, предназначенных для управления плановой n-го вида деятельностью в m-ой организационной системе;

– данные $W^{nm}{}_{\text{план.}}$ о множестве плановых сценариев, предназначенных для управления плановой n-го вида деятельностью в m-ой организационной системе при условии $\Delta S_{nm\text{-доп.}} \le \Delta S^*_{nm} < 1$, при этом

$W^{nm}{}_{\text{план.}} = \{W^{nm1}{}_{\text{план.}}$ или $W^{nm2}{}_{\text{план.}} \ldots$ или $W^{nmYnm\text{-план.}}{}_{\text{план.}}\}$, где

$W^{nmy3}{}_{\text{план.}}$ – данные о $y3$-ом плановом сценарии, предназначенном для управления плановой n-го вида деятельностью в m-ой организационной системе,

$y3$ – данные о приоритете планового сценария;

$y3 = 1, 2, \ldots, Y_{nm\text{-план.}}$, при этом выполняется условие

$P(W^{nmy3}{}_{\text{план.}}) \geq P(W^{nm(y3\text{-}1)}{}_{\text{план.}})$, $\sum_{y3=1}^{Y_{nm-план.}} P(W^{nmy3}_{план.}) = 1$, где

$P(W^{nmy3}{}_{\text{план.}})$ и $P(W^{nm(y3\text{-}1)}{}_{\text{план.}})$ – соответственно данные о прогнозируемых вероятностях для выбора планового сценария $W^{nmy3}{}_{\text{план.}}$ и планового сценария $W^{nm(y3\text{-}1)}{}_{\text{план.}}$, $P(W^{nm0}{}_{\text{план.}})=0$.

Перечисленные выше данные о сценариях управления хранятся в системе хранения данных, периодически подвергаются аудиту и обновляются. Производится разработка новых данных о сценариях управления и их размещение в системе хранения данных аудита деятельности организационных систем.

Разработка новых данных о сценариях управления производится в следующих случаях:

– если в результате анализа данных об эффективности деятельности организационной системы в системе хранения данных отсутствуют данные о сценарии управления, соответствующем данным о существующей ситуации в рассматриваемом временном интервале, причём данные о ситуации – это совокупность данных о событиях, состояниях объектов, о силах и средствах, данные о других сущностях, которые оказывают влияние на деятельность организационных систем (ОС) в рассматриваемом временном интервале;
– если в результате проведения операций по проверке актуальности данных об уже выбранном для исполнения сценарии управления, было произведено переформирование этих данных и, тем самым, сформированы новые данные о сценарии управления.

На рис. 2 отображена схема направлений управляющих воздействий (команд управления) системы управления деятельностью ОС на объекты наблюдения, которые оказывают влияние на деятельность ОС. На рис. 3 приведена структурная схема преобразователя 5 данных системы управления деятельностью ОС. В состав преобразователя 5 данных входят комплекс 5.1 кодирования информации и средства 5.2.1 – 5.2.*R* связи.

При этом первые вход и выход преобразователя 5 данных являются соответственно первыми входом и выходом комплекса 5.1 кодирования информации, вторые входы и выходы которого соединены каждый соответственно с первыми выходом и входом одного из средств 5.2.1 – 5.2.*R* связи, вторые выход и вход каждого из которых являются соответственно одними из вторых выходов и входов преобразователя 5 данных.

Функционирование системы. Система управления деятельностью организационных систем работает следующим образом.

В исходном состоянии в вычислительном комплексе 1.1 формируются и запоминаются технологические данные, в том числе данные о требуемых показателях объектов наблюдения. Перечень данных приведён выше при описании технического решения.

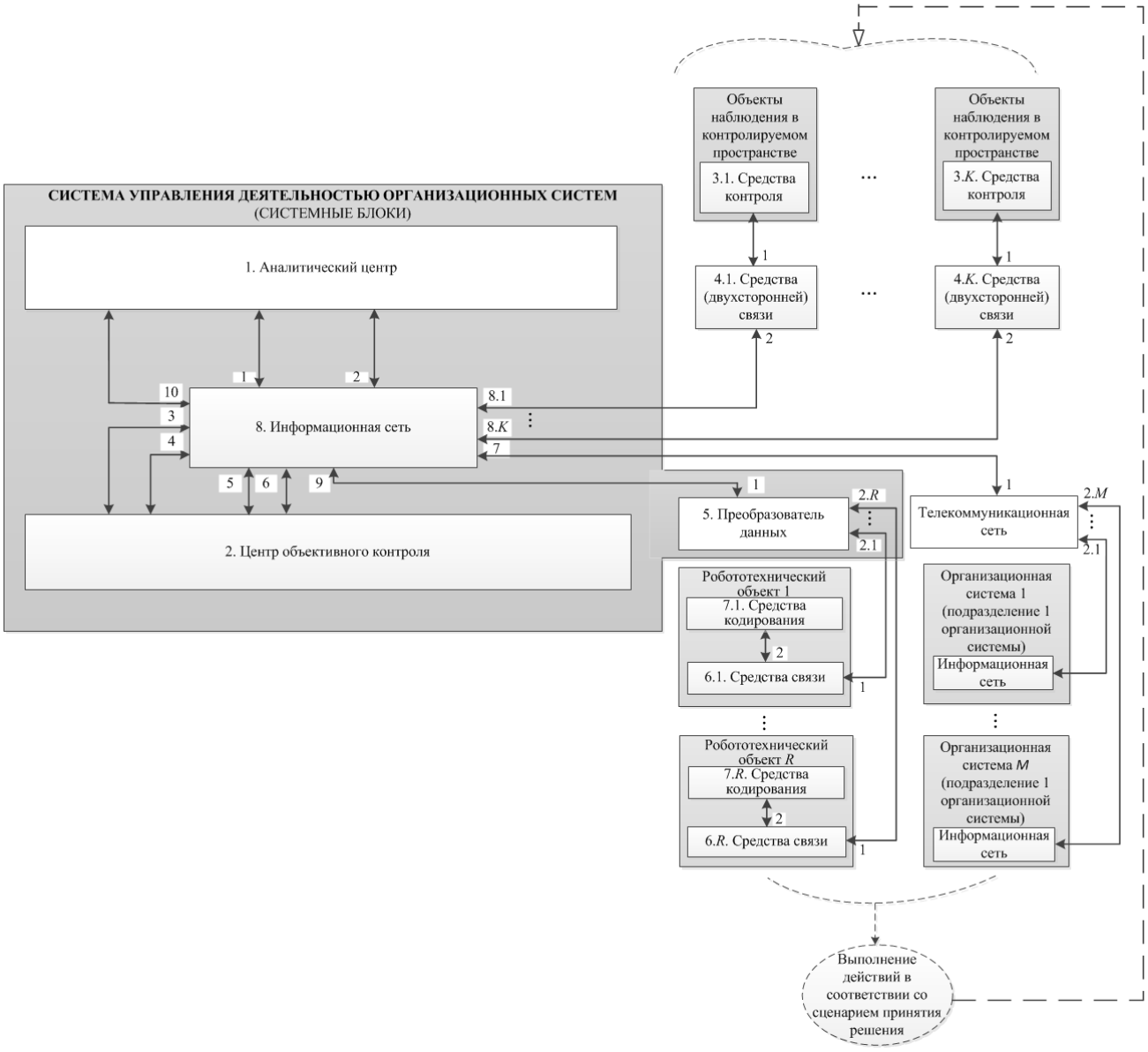


Рис. 2. Схема управляющих воздействий системы управления деятельностью организационных систем на объекты влияния (объекты наблюдения)

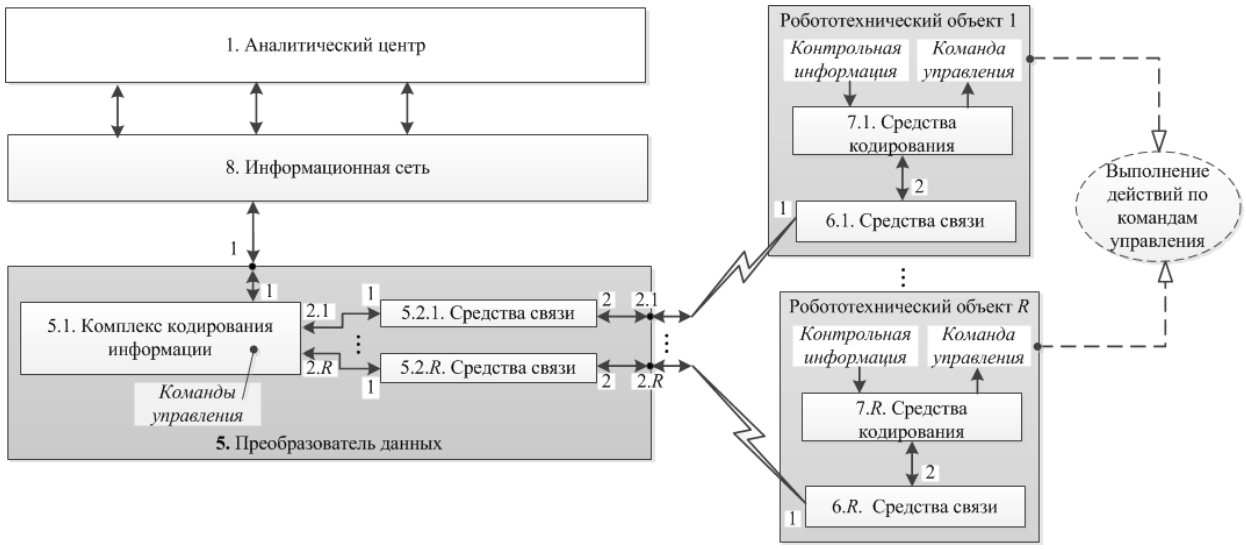


Рис. 3. Структурная схема преобразователя данных

Средства 3.1 – 3.*K* контроля над объектами наблюдения производят сбор данных о фактических показателях объектов наблюдения, представленных безразмерными числами и/или единицами измерений. Передача этих данных из средств 3.1 – 3.*K* контроля в вычислительный комплекс 1.1 осуществляется с помощью средств 4.1 – 4.*K* связи и информационной сети 8.

В вычислительном комплексе 1.1 производится:

- обработка данных о требуемых и фактических показателях объектов наблюдения;
- выработка данных о фактических состояниях объектов наблюдения, о фактическом состоянии видов деятельности и о фактическом состоянии деятельности организационных систем (их подразделений) в целом;
- анализ эффективности деятельности организационных систем.

В зависимости от результатов анализа эффективности деятельности в вычислительном комплексе 1.1:

- производится выбор из числа данных о сценариях управления, которые записаны в системе 1.2 хранения данных, данные о сценарии, который непосредственно может быть использован в сложившейся ситуации для управления объектом (объектами) наблюдения с помощью робототехнического объекта (объектов) и/или информационной сети (сетей) организационной системы (систем, их подразделений);
- выбранные данные о сценарии управления передаются в комплекс 1.3 средств аудита для проверки их актуальности – проведения целевого аудита данных.

В состав данных о сценарии управления входят данные, необходимые для выполнения работ в соответствии с этим сценарием – данные обо всех сущностях, необходимых для производства управляющих воздействий над объектами наблюдения и для управления робототехническими объектами. По меньшей мере, это данные:

- о робототехнических объектах, которые должны произвести действия над объектами наблюдения и другими объектами (при автоматическом управлении), об объектах наблюдения, над которыми должны быть проведены необходимые действия (при автоматическом и автоматизированном управлении);
- для настройки программных средств, администрирования аппаратных средств и средств защиты от опасных программно-технических воздействий из состава средств, обеспечивающих деятельность организационных систем (при автоматическом и автоматизированном управлении);
- о силах и средствах организационных систем, требуемых для реализации сценариев управления (при автоматизированном управлении), а также другие данные, которые необходимы для выполнения действий по устранению угроз различного характера, по

их предотвращению или по выполнению плановых работ, включая данные о силах организационных систем, привлекаемых к работам.

Целевой аудит данных о выбранном сценарии управления (например, о сценарии *S*) проводится с целью определения достоверности этих данных. При этом на примере данных о выбранном сценарии управления *S*, производятся следующие действия:

- целевой аудит данных, относящихся к сценарию *S*, который выполняется на базе вычислительного комплекса 1.1, системы 1.2 хранения данных, комплекса 1.3 средств аудита и комплекса 1.4 средств моделирования, при этом осуществляется сбор фактических данных, относящихся к сценарию *S*, сравнительный анализ этих данных с данными об информационных моделей, хранящимися в комплексе 1.4 средств моделирования;
- в случае если изменений в данных о сценарии *S*, не обнаружено, то данные об этом сценарии передаются в робототехнические объекты и/или информационные сети организационных систем для исполнения управляющих воздействий над объектами наблюдения, адресные данные, данные об управляющих воздействий (команды управления, настроечные данные и др.) и другие данные, необходимые для производства управляющих воздействий, входят в состав данных о выбранном сценарии управления.

В случае если обнаружены изменения в данных о сценарии *S*, то выполняются следующие действия:

- модернизация информационных моделей, относящихся к сценарию *S*;
- переформирование данных о сценарии *S* на основе модернизированных информационных моделей – формирование данных о сценарии S^M;
- передача данных о сценарии S^M для производства управляющих воздействий в робототехнические объекты и/или в информационные сети организационных систем.

На рис. 4 приведён граф-схема алгоритма функционирования системы управления деятельностью организационных систем, с учётом действий по проверке актуальности данных о выбранном сценарии управления. Данный граф иллюстрирует описанные выше действия.

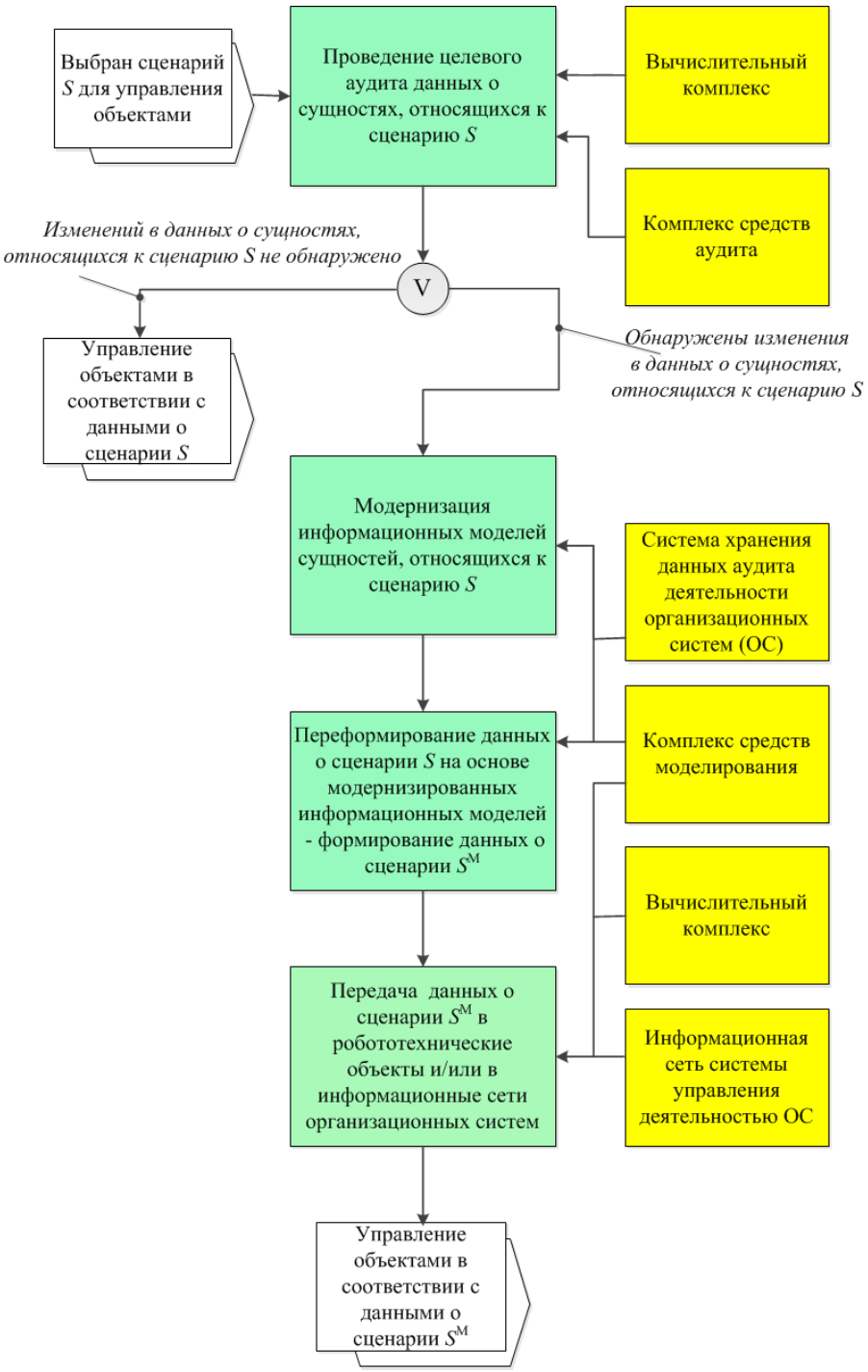


Рис. 4. Граф-схема алгоритма управления объектами (робототехническими объектами и другими объектами наблюдения) с учётом результатов проверки актуальности данных

Для обмена данными с помощью информационной сети 8, телекоммуникационной сети организационных систем и средств связи образуются следующие типы трактов передачи данных (информационных трактов):

- тракты передачи данных с видеоизображениями между вычислительным комплексом 1.1 и видеосистемой 2.3.1 (рис. 5);
- тракты передачи данных между вычислительным комплексом 1.1 и информационными сетями организационных систем (рис. 6);

Рис. 5. Тракты передачи данных – с видеоизображениями, между вычислительным комплексом и видеосистемой (пример 1)

Рис. 6. Тракты передачи данных – между вычислительным комплексом и информационными сетями организационных систем (пример 2)

– тракты передачи данных с исчисляемыми показателями, между средствами 3.1 – 3.*K* контроля над объектами наблюдений и вычислительным комплексом 1.1 (рис. 7);
– тракты передачи данных с видеоизображениями между средствами 3.1 – 3.*K* контроля над объектами наблюдений и мультимедиа – проектора 2.2.2 с экраном (рис. 8).

Рис. 7. Тракты передачи данных – с исчисляемыми показателями, между средствами контроля и вычислительным комплексом (пример 3)

Рис. 8. Тракты передачи данных – с видеоизображениями между средствами контроля и мультимедиа – проектором с экраном (пример 4)

Реализация компонентов системы. Вычислительный комплекс 1.1, комплекс 1.4 средств моделирования, видеосистема 2.3.1 с компьютером 2.3.2 настройки видеосистемы (рис. 1) могут быть выполнены на основе общеизвестных промышленных аппаратных и программных средств вычислительной техники и видео. На рис. 9 – рис. 14 приведены примеры граф-схем алгоритмов (ГСА), которые отражают логику действий технического решения и показывают возможность их реализации с помощью простых операций в указанных выше компонентах системы управления деятельностью организационных систем.

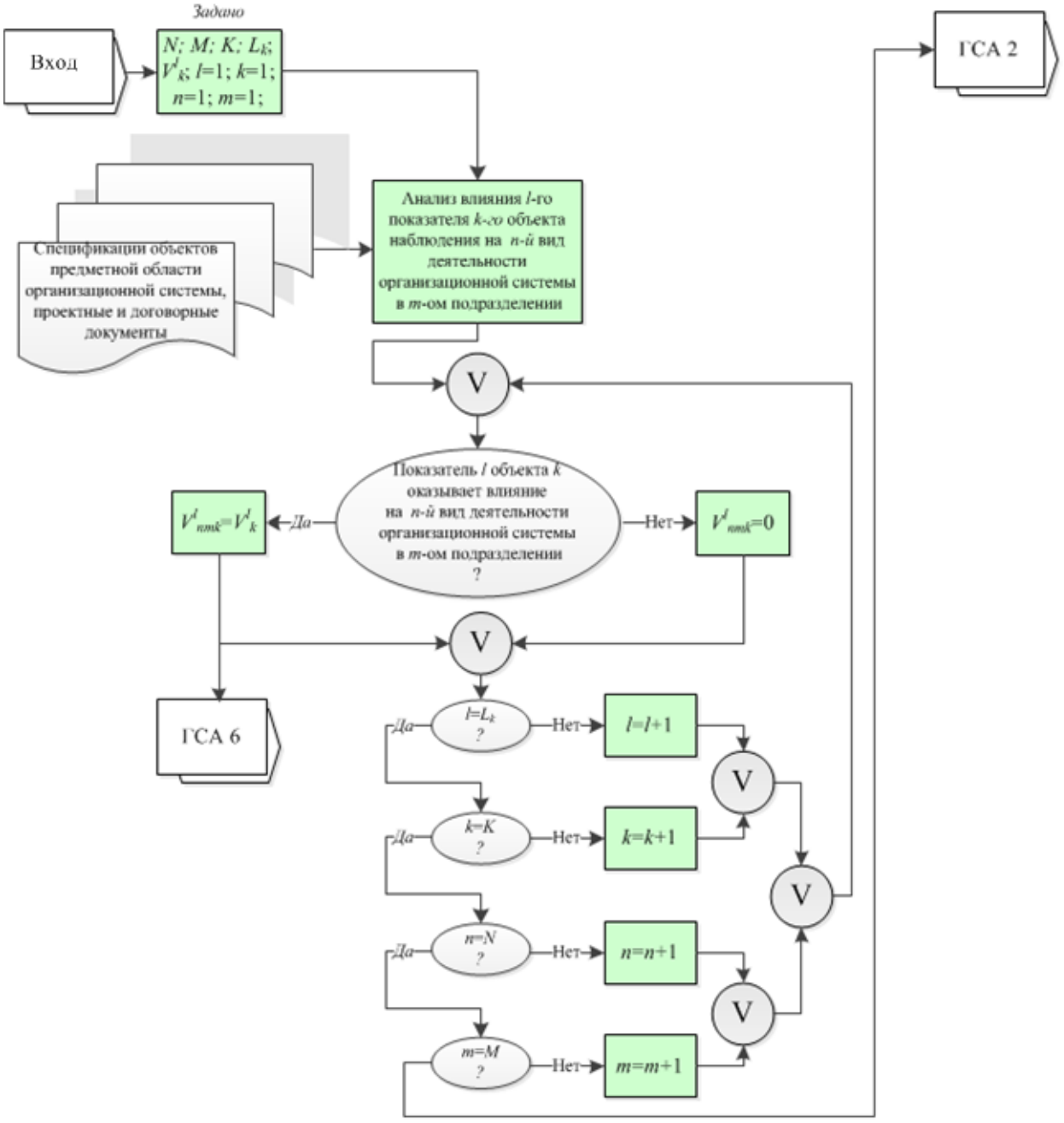


Рис. 9. Граф-схема алгоритма 1 (ГСА 1). Формирование блока данных V^l_{nmk} о требуемом l-ом показателе состояния k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ом подразделении организационной системы, где l=1, 2, …, $L(k)$; n=1, 2, …, N; m=1, 2, …, M; k=1, 2, …, K.

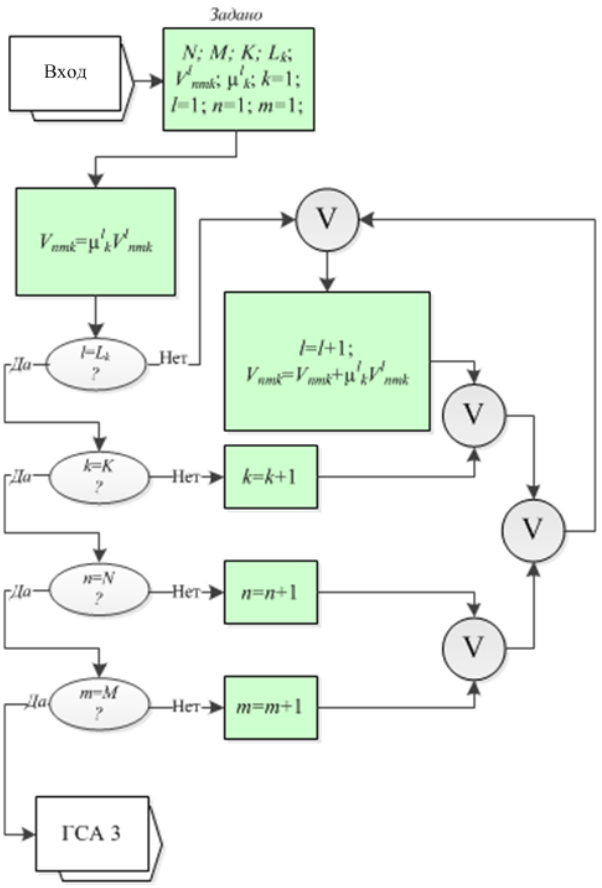


Рис. 10. Граф-схема алгоритма 2 (ГСА 2). Формирование блока данных V_{nmk} о требуемом состоянии k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ом подразделении организационной системы, где n=1, 2, …, N; m=1, 2, …, M; k=1, 2, …, K.

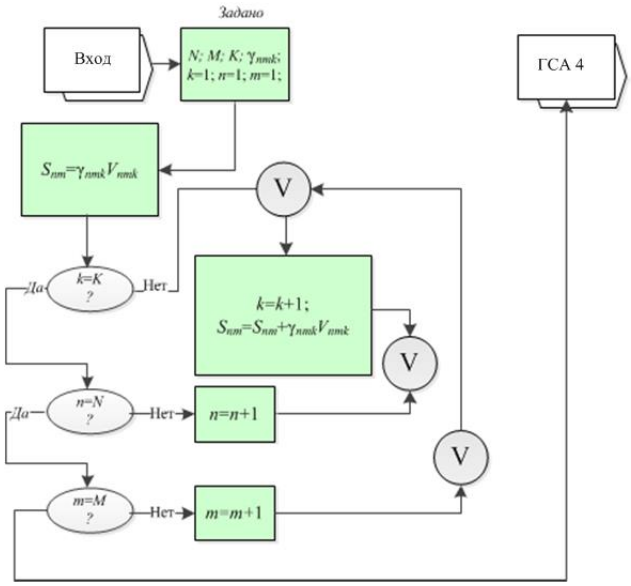


Рис. 11. Граф-схема алгоритма 3 (ГСА 3). Формирование блока данных S_{nm} о требуемом состоянии n-го вида деятельности, осуществляемой в m-ом подразделении организационной системы, n=1, 2, …, N; m=1, 2, …, M.

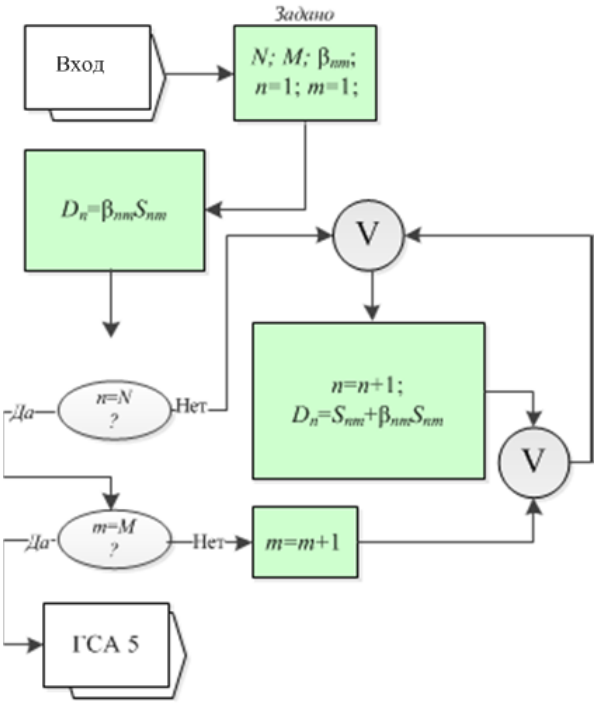


Рис. 12. Граф-схема алгоритма 4 (ГСА 4). Формирование блока данных D_n – о требуемом состоянии n-го вида деятельности организационной системы, где n=1, 2, …, N

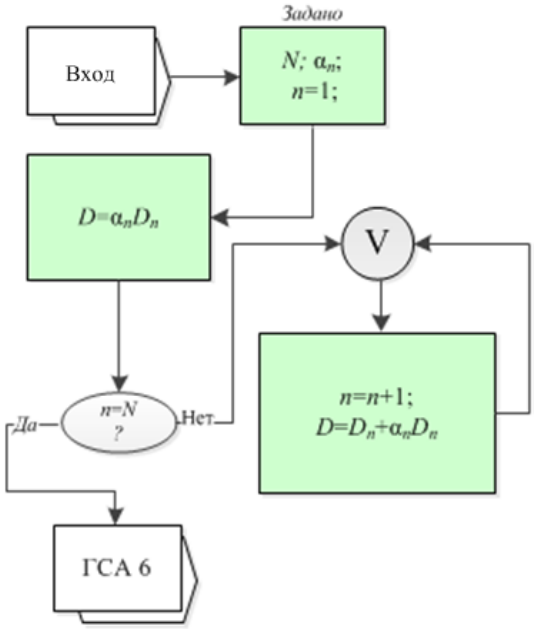


Рис. 13. Граф-схема алгоритма 5 (ГСА 5). Формирование блока данных D о требуемом состоянии деятельности организационной системы в целом

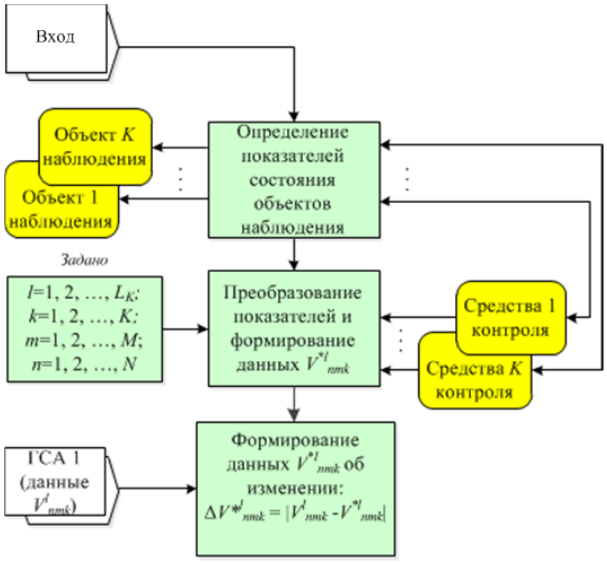


Рис. 14. Граф-схема алгоритма 6 (ГСА 6). Формирование данных об абсолютном значении отклонения данных V^{*l}_{nmk} фактического l показателя k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ом подразделении организационной системы, от требуемых данных V^{l}_{nmk}

По аналогии с граф-схемами алгоритмов, приведённых на рис. 9 – рис. 14, строятся граф-схемы алгоритмов для преобразования других данных заявляемого технического решения, приведённых ниже в таблице.

Обозначения		***Определения и формулы***
k=1, 2, …, K	–	данные о порядковом номере объекта наблюдения.
l=1, 2, …, $L(k)$	–	данные о порядковом номере показателя k-го объекта наблюдения.
n=1, 2, …, N	–	данные о порядковом номере вида деятельности организационных систем.
m=1, 2, …, M	–	данные о порядковом номере организационной системы (подразделения).
K	–	данные о числе объектов наблюдения в контролируемом пространстве организационных систем.
$L(k)$	–	данные о числе показателей k-го объекта наблюдения.
N	–	данные о числе контролируемых видов деятельности организационных систем.
M	–	данные о числе организационных системы (подразделений).
μ^{l}_{k}	–	данные о приоритете l-ого показателя k-го объекта наблюдения.
γ_{nmk}	–	данные о приоритете k-го объекта наблюдения, который оказывает влияние на n-ый вид деятельности, осуществляемой в m-ой организационной системе (подразделении).
α_{n}	–	данные о приоритете n-го вида деятельности организационной системы.
β_{nm}	–	данные о приоритете n-го вида деятельности, осуществляемой в m-ой организационной системе (подразделении).
V^{l}_{k}	–	данные о требуемом (проектном значении, заданном) l-ом показателе k-го объекта наблюдения.

Обозначения		*Определения и формулы*
V^{l}_{nmk}	–	данные о требуемом *l*-ом показателе *k*-го объекта наблюдения, с учётом его влияния на состояние *n*-ой деятельности в *m*-ой организационной системе (подразделении).
V_{nmk}	–	данные о требуемом состоянии *n*-го вида деятельности, осуществляемой в *m*-ой организационной системе (подразделении), обусловленном *k*-ым объектом наблюдения:
$V_{nmk} = \mu^{1}_{k} V^{1}_{nmk} + \mu^{2}_{k} V^{2}_{nmk}, +\ldots+ \mu^{L(k)}_{k} V^{L(k)}_{nmk}.$		
V^{*l}_{nmk}	–	данные о фактическом *l* показателе *k*-го объекта наблюдения, который оказывает влияние на *n*-ый вид деятельности, осуществляемой в *m*-ой организационной системе (подразделении) (выработаны средствами контроля над объектами наблюдения).
ΔV^{*l}_{nmk}	–	данные об абсолютном значении отклонения данных V^{*l}_{nmk} фактического *l* показателя *k*-го объекта наблюдения, который оказывает влияние на *n*-ый вид деятельности, осуществляемой в *m*-ой организационной системе (подразделении), от данных V^{l}_{nmk} о требуемом *l* показателе *k*-го объекта наблюдения, который оказывает влияние на *n*-ый вид деятельности, осуществляемой в *m*-ой организационной системе (подразделении):
$\Delta V^{*l}_{nmk} = \lvert V^{l}_{nmk} - V^{*l}_{nmk} \rvert.$		
V^{*}_{nmk}	–	данные о фактическом состоянии *k*-го объекта наблюдения, который оказывает влияние на *n*-ый вид деятельности, осуществляемой в *m*-ой организационной системе (подразделении):
$V^{*}_{nmk} = \mu^{1}_{k} (V^{1}_{nmk} - \Delta V^{*1}_{nmk}) + \mu^{2}_{k} (V^{2}_{nmk} - \Delta V^{*2}_{nmk}) + \ldots + \mu^{L(k)}_{k} (V^{L(k)}_{nmk} - V^{*L(k)}_{nmk}).$		
S_{nm}	–	данные о требуемом состоянии *n*-го вида деятельности, осуществляемой в *m*-ой организационной системе (подразделении):
$S_{nm} = \gamma_{nm1} V_{nm1} + \gamma_{nm2} V_{nm2} +\ldots+ \gamma_{nmK} V_{nmK}.$		
S^{*}_{nm}	–	данные о фактическом состоянии *n*-го вида деятельности, осуществляемой в *m*-ой организационной системе (подразделении):
$S^{*}_{nm} = \gamma_{nm1} V^{*}_{nm1} + \gamma_{nm2} V^{*}_{nm2} +\ldots+ \gamma_{nmK} V^{*}_{nmK}.$		
ΔS^{*}_{nm}	–	данные о фактическом показателе эффективности *n*-го вида деятельности в *m*-ой организационной системе (подразделении):
$\Delta S^{*}_{nm} = S^{*}_{nm} / S_{nm}.$		
$\Delta S_{nm\text{-крит.}}$	–	данные о критическом показателе эффективности *n*-го вида деятельности в *m*-ой организационной системе (подразделении), снижение, по сравнению с которым, фактического показателя ΔS^{*}_{nm} эффективности *n*-го вида деятельности в *m*-ой организационной системе (подразделении) означает существование угрозы для этого вида деятельности в *m*-ой организационной системе (подразделении) и необходимости принятия действий по её устранению:
$\Delta S_{nm\text{-крит.}} < 1,$ например, $\Delta S_{nm\text{-крит.}} = 0{,}5.$		
$W_{nm\text{-крит.}}$	–	данные о множестве критических сценариев управления, предназначенных для устранения угрозы для *n*-го вида деятельности в *m*-ой организационной системе (подразделении):
$W_{nm\text{-крит.}} = \{W^{1}_{nm\text{-крит.}}$ или $W^{2}_{nm\text{-крит.}} \ldots$ или $W^{Ynm\text{-крит.}}_{nm\text{-крит.}}\},$ рекомендуются для управления при условии: $0 \le \Delta S^{*}_{nm} < \Delta S_{nm\text{-крит.}}$		
$W^{y1}_{n\text{-крит.}}$	–	данные о *y*1-ом критическом сценарии управления, предназначенном для устранения угрозы для *n*-го вида деятельности в *m*-ой организационной системе (подразделении).

Обозначения		*Определения и формулы*
$y1$	–	данные о приоритете $y1$-го критического сценария, где
$y1=1, 2, \ldots, Y_{nm\text{-крит.}}$, чем меньше $y1$, тем выше приоритет сценария.		
$Y_{nm\text{-крит.}}$	–	данные о числе критических сценариев управления, предназначенных для устранения угрозы для n-го вида деятельности в m-ой организационной системе (подразделении).
$\Delta S_{nm\text{-доп.}}$	–	данные о допустимом показателе эффективности n-го вида деятельности в m-ой организационной системе (подразделении), снижение, по сравнению с которым фактического показателя ΔS^*_{nm} эффективности n-го вида деятельности в m-ой организационной системе (подразделении) означает возможность появления угрозы для этого вида деятельности в m-ой организационной системе (подразделении) и необходимости принятия действий по недопущению её появления:
$\Delta S_{nm\text{-доп.}} <1$, например, $\Delta S_{nm\text{-доп.}}=0{,}9$.		
$W_{nm\text{-пред.}}$	–	данные о множестве предупреждающих сценариев управления, предназначенных для предотвращения угрозы для n-го вида деятельности в m-ой организационной системе (подразделении):
$W_{nm\text{-пред.}}= \{W^1_{nm\text{-пред.}}$ или $W^2_{nm\text{-пред.}} \ldots$ или $W^{Ynm\text{-пред.}}_{nm\text{-пред.}}\}$, рекомендуются для управления при условии: $\Delta S_{nm\text{-крит.}} \le \Delta S^*_{nm} < \Delta S_{nm\text{-доп.}}$		
$W^{y2}_{nm\text{-пред.}}$	–	данные о $y2$-ом предупреждающем сценарии управления, предназначенном для предотвращения угрозы для n-го вида деятельности в m-ой организационной системе (подразделении).
$y2$	–	данные о приоритете $y2$-го предупреждающего сценария, где
$y2=1, 2, \ldots, Y_{nm\text{-пред.}}$, чем меньше $y2$, тем выше приоритет сценария.		
$Y_{nm\text{-пред.}}$	–	данные о числе предупреждающих сценариев управления, предназначенных для предотвращения угрозы для n-го вида деятельности в m-ой организационной системе (подразделении).
$W_{nm\text{-план.}}$	–	данные о множестве плановых сценариев управления, предназначенных для повышения эффективности n-го вида деятельности в m-ой организационной системе (подразделении):
$W_{nm\text{-план.}} = \{W^1_{nm\text{-план.}}$ или $W^2_{nm\text{-план.}} \ldots$ или $W^{Ynm\text{-план.}}_{nm\text{-план.}}\}$, рекомендуются для управления при условии: $\Delta S_{nm\text{-доп.}} \le \Delta S^*_{nm} <1$.		
$W^{y3}_{nm\text{-план.}}$	–	данные о $y3$-ом плановом сценарии управления, предназначенном для повышения эффективности n-го вида деятельности в m-ой организационной системе (подразделении).
$y3$	–	данные о приоритете $y3$-го планового сценария, где
$y3=1, 2, \ldots, Y_{nm\text{-план.}}$, чем меньше $y3$, тем выше приоритет сценария.		
$Y_{nm\text{-план.}}$	–	данные о числе плановых сценариев управления, предназначенных для повышения эффективности n-го вида деятельности в m-ой организационной системе (подразделении).
D_n	–	данные о требуемом состоянии n-го вида деятельности организационных систем:
$D_n = \beta_{n1}S_{n1} + \beta_{n2}S_{n2}, + \ldots + \beta_{nM}S_{nM}$.		

Обозначения		*Определения и формулы*
D^*_n	–	данные о фактическом состоянии n-го вида деятельности организационных систем:
$D^*_n = \beta_{n1}S^*_{n1} + \beta_{n2}S^*_{n2} + \ldots + \beta_{nM}S^*_{nM}$.		
ΔD^*_n	–	данные о фактическом показателе эффективности n-го вида деятельности организационных систем:
$\Delta D^*_n = D^*_n / D_n$.		
$\Delta D_{n\text{-крит.}}$	–	данные о критическом показателе эффективности n-го вида деятельности организационных систем, снижение, по сравнению с которым, фактического показателя ΔD^*_n эффективности n-го вида деятельности организационных систем означает существование угрозы для этого вида деятельности организационных систем и необходимости принятия действий по недопущению её появления:
$\Delta D_{n\text{-крит.}} < 1$, например, $\Delta D_{n\text{-крит.}} = 0{,}5$.		
$W_{n\text{-крит.}}$	–	данные о множестве критических сценариев управления, предназначенных для устранения угрозы для n-го вида деятельности организационных систем:
$W_{n\text{-крит.}} = \{W^1{}_{n\text{-крит.}}$ или $W^2{}_{n\text{-крит.}}$ … или $W^{Un\text{-крит.}}{}_{n\text{-крит.}}\}$, рекомендуются для управления при условии: $0 \le \Delta D_n^* < \Delta D_{n\text{-крит.}}$		
$W^{u1}{}_{n\text{-крит.}}$	–	данные о $u1$-ом критическом сценарии управления, предназначенных для устранения угрозы для n-го вида деятельности организационных систем.
$u1$	–	данные о приоритете $u1$-го критического сценария, где
$u1=1, 2, \ldots, U_{n\text{-крит.}}$, чем меньше $u1$, тем выше приоритет сценария.		
$U_{n\text{-крит.}}$	–	данные о числе критических сценариях управления, предназначенных для устранения угрозы для n-го вида деятельности организационных систем.
$\Delta D_{n\text{-доп.}}$	–	данные о допустимом показателе эффективности n-го вида деятельности организационных систем, снижение, по сравнению с которым, фактического показателя ΔD^*_n эффективности n-го вида деятельности организационных систем означает возможность появления угрозы для этого вида деятельности организационных систем и необходимости принятия действий по недопущению её появления:
$\Delta D_{n\text{-крит.}} < \Delta D_{n\text{-доп.}} < 1$, например, $\Delta D_{n\text{-доп.}} = 0{,}9$.		
$W_{n\text{-пред.}}$	–	данные о множестве предупреждающих сценариев управления, предназначенных для предотвращения угрозы для n-го вида деятельности организационных систем:
$W_{n\text{-пред.}} = \{W^1{}_{n\text{-пред.}}$ или $W^2{}_{n\text{-пред.}}$ … или $W^{Un\text{-пред.}}{}_{n\text{-пред.}}\}$, рекомендуются для управления при условии: $\Delta D_{n\text{-крит.}} \le \Delta D_n^* < \Delta D_{n\text{-доп.}}$		
$W^{u2}{}_{n\text{-пред.}}$	–	данные о $u2$-ом предупреждающем сценарии управления, предназначенном для предотвращения угрозы для n-го вида деятельности организационных систем.
$u2$	–	данные о приоритете $u2$-го предупреждающего сценария, где
$u2=1, 2, \ldots, U_{n\text{-пред.}}$, чем меньше $u2$, тем выше приоритет сценария.		

Обозначения		*Определения и формулы*
$U_{n\text{-пред.}}$	–	данные о числе предупреждающих сценариев управления, предназначенных для предотвращения угрозы для *n*-го вида деятельности организационных систем.
$W_{n\text{-план.}}$	–	данные о множестве плановых сценариев управления, предназначенных для повышения эффективности *n*-го вида деятельности организационных систем:
$W_{n\text{-план.}} = \{W^1_{n\text{-план.}}$ или $W^2_{n\text{-план.}} \ldots$ или $W^{Un\text{-план.}}_{n\text{-план.}}\}$, рекомендуются для управления при условии: $\Delta D_{n\text{-крит.}} \leq \Delta D_n^* < 1$.		
$W^{u3}_{n\text{-план.}}$	–	данные о *u*3-ом плановом сценарии управления, предназначенном для повышения эффективности *n*-го вида деятельности организационных систем.
*u*3	–	данные о приоритете *u*3-го планового сценария, где
$u3=1, 2, \ldots, U_{n\text{-план.}}$, чем меньше *u*3, тем выше приоритет сценария.		
$U_{n\text{-план.}}$	–	данные о числе плановых сценариев управления, предназначенных для повышения эффективности *n*-го вида деятельности организационных систем.
D	–	данные о требуемом состоянии деятельности организационных систем в целом:
$D = \alpha_1 D_1 + \alpha_2 D_2 + \ldots + \alpha_N D_N$.		
*D**	–	данные о фактическом состоянии деятельности организационных систем в целом:
$D^* = \alpha_1 D^*_1 + \alpha_2 D^*_2 + \ldots + \alpha_N D^*_N$.		
ΔD^*	–	данные о показателе эффективности деятельности организационных систем в целом:
$\Delta D^* = D^*/ D$.		
$\Delta D_{крит.}$	–	данные о критическом показателе эффективности деятельности организационных систем в целом, снижение, по сравнению с которым, фактического показателя ΔD^* эффективности деятельности организационных систем в целом означает существование угрозы для деятельности организационных систем в целом и необходимости принятия действий по её устранению:
$\Delta D_{крит.} < 1$, например, $\Delta D_{крит.} = 0{,}5$.		
$W_{крит.}$	–	данные о множестве критических сценариев управления, предназначенных для устранения угрозы для деятельности организационных систем в целом:
$W_{крит.} = \{W^1_{крит.}$ или $W^2_{крит.} \ldots$ или $W^{Qкрит.}_{крит.}\}$, рекомендуются для управления при условии: $0 \leq \Delta D^* < \Delta D_{крит.}$		
$W^{q1}_{крит.}$	–	данные о *q*1-ом критическом сценарии управления, предназначенном для устранения угрозы для деятельности организационных систем в целом.
*q*1	–	данные о приоритете *q*1-го критического сценария, где
$q1=1, 2, \ldots, Q_{крит.}$, чем меньше *q*1, тем выше приоритет сценария.		
$Q_{крит.}$	–	данные о числе критических сценариях управления, предназначенных для устранения угрозы для деятельности организационных систем в целом.

Обозначения		*Определения и формулы*
$\Delta D_{доп.}$	–	данные о допустимом показателе эффективности деятельности организационной системы в целом, снижение, по сравнению с которым, фактического показателя означает возможность появления угрозы для деятельности организационных систем в целом и необходимости принятия действий по недопущению её появления.
$\Delta D_{крит.} < \Delta D_{доп.} < 1$, например, $\Delta D_{доп.}=0{,}9$.		
$W_{пред.}$	–	данные о множестве предупреждающих сценариев управления, предназначенных для предотвращения угрозы для деятельности организационных систем в целом:
$W_{пред.}= \{W^1_{пред.}$ или $W^2_{пред.}$ … или $W^{Qпред.}_{пред.}\}$, рекомендуются для управления при условии: $\Delta D_{крит.} \le \Delta D^* < \Delta D_{доп.}$		
$W^{q2}_{пред.}$	–	данные о $q2$-ом предупреждающем сценарии управления, предназначенном для предотвращения угрозы для деятельности организационных систем в целом.
$q2$	–	данные о приоритете $q2$-го предупреждающего сценария, где
$q2=1, 2, \ldots, Q_{пред.}$, чем меньше $q2$, тем выше приоритет сценария.		
$Q_{пред.}$	–	данные о числе предупреждающих сценариев управления, предназначенных для предотвращения угрозы для деятельности организационных систем в целом.
$W_{план.}$	–	данные о множестве плановых сценариев управления, предназначенных для повышения эффективности деятельности организационных систем в целом:
$W_{план.} = \{W^1_{план.}$ или $W^2_{план.}$ … или $W^{Qплан.}_{план.}\}$, рекомендуются для управления при условии: $\Delta D_{доп.} \le \Delta D^* < 1$.		
$W^{q3}_{план.}$	–	данные о $q3$-ом плановом сценарии управления, предназначенном для повышения эффективности деятельности организационных систем в целом.
$q3$	–	данные о приоритете $q3$-го планового сценария, где
$q3=1, 2, \ldots, Q_{план.}$, чем меньше $q3$, тем выше приоритет сценария.		
$Q_{план.}$	–	данные о числе плановых сценариях управления, предназначенных для повышения эффективности деятельности организационных систем в целом.

В качестве логической основы системы управления деятельностью организационных систем [4] используется техническое решение «Способ поддержки деятельности организационной системы» [7].

Способ поддержки деятельности организационной системы

Техническое решение «Способ поддержки деятельности организационной системы» [7] относится к области подготовки информации для управления деятельностью организационных систем. Предметной областью является подготовка информации для принятия и исполнения решений по управлению объектами наблюдения в контролируемом пространстве и во внешней среде, включая информационные системы и сети, робототехнические объекты,

которые оказывают влияние на состояние деятельности организационных систем.

В настоящее время создаются организационно-технические системы различного назначения, направленные на повышение эффективности процессов управления в организационных системах различных типов. При этом автоматизируются практически все виды деятельности организационных систем – предприятий, организаций, корпораций, государственных структур. Одной из острейших проблем, которые необходимо решать при создании и дальнейшем функционировании таких систем, является постоянный рост объемов информации, необходимой для решения различных задач. Каким образом обеспечить эффективное использование всех имеющихся технических возможностей и накопленных информационных ресурсов? Каким образом оперативно и достаточно точно решать возникающие задачи на основе использования интегрального информационного ресурса? Подобных вопросов возникает достаточно много. Все они связаны с поиском необходимой информации, ее анализом, выработкой сценариев для принятия решения, выбором наиболее эффективного из них с учетом оценки возможных рисков и принятием решения на его реализацию. С обеспечением условий для качественного и своевременного выполнения решения. Для получения ответов на эти и другие аналогичные вопросы разрабатывают инновационные технические решения – как способы, так и устройства, системы, связанные с повышением эффективности управленческих процессов. Предлагают технические решения, которые относятся к таким системам, как «ситуационный центр», «аналитический центр», «система объективного контроля ситуации», «автоматизированная система поддержки принятия решений», «информационно-аналитическая система лица, принимающего решения» и другие. Все эти решения можно отнести к одной области техники – к области деятельности организационной системы, осуществляемой с применением объектов поддержки (наблюдения) в контролируемом пространстве и во внешней среде, которые оказывают влияние на состояние деятельности организационных систем. При этом основными показателями для оценки эффективности организационных систем становятся показатели эффективности их деятельности, а данные о показателях состояния объектов поддержки (наблюдения) являются исходными для определения основных показателей.

Технической задачей, на решение которой направлено техническое решение «Способ поддержки деятельности организационной системы» [7], является предложение нового и улучшенного способа поддержки деятельности организационной системы, способного предотвратить или сократить сроки разрешения сложных проблемных ситуаций в деятельности организационной системы и привести её в допустимое нормативами состояние.

Способ поддержки деятельности организационной системы *характеризуется* тем, что содержит этапы, на которых с помощью средств контроля, средств управления, телекоммуникационной сети и аппаратно-программных средств центра управления, ситуационно-аналитических центров и пунктов управления подразделений организационной системы:

1. Формируют блоки данных:
- о нормированных показателях объектов поддержки;
- о нормированных состояниях объектов поддержки с учётом их влияния на виды деятельности в подразделениях организационной системы;
- о нормированных состояниях видов деятельности в подразделениях организационной системы, видов деятельности и деятельности организационной системы в целом;
- о критических и допустимых показателях эффективности видов деятельности в подразделениях организационной системы, видов деятельности и деятельности организационной системы в целом;
- о командах управления, предназначенных для установления объектов поддержки организационной системы в нормированные и/или допустимые состояния с учётом их влияния на виды деятельности подразделений организационной системы, на виды деятельности организационной системы и на деятельность организационной системы в целом, в зависимости от фактической ситуации.

2. Устанавливают объекты поддержки организационной системы в нормированные состояния с учётом их влияния на виды деятельности в подразделениях организационной системы, виды деятельности и деятельность организационной системы в целом.

3. Определяют фактические показатели объектов поддержки организационной системы.

4. Формируют блоки данных о фактических показателях и состояниях объектов поддержки организационной системы с учётом их влияния на виды деятельности в подразделениях организационной системы, о фактических состояниях видов деятельности в подразделениях организационной системы, видов деятельности и деятельности организационной системы в целом.

5. Производят на основе сформированных данных оценку фактической эффективности:
- видов деятельности в подразделениях организационной системы;
- видов деятельности организационной системы;
- деятельности организационной системы в целом.

6. Определяют на основе результатов оценки из числа сформированных блоков данных о командах управления блоки данных о командах управления, которые предназначены для установления объектов поддержки организационной системы в допустимые состояния.

7. Устанавливают объекты поддержки организационной системы в допустимые состояния с учётом их влияния:
- на виды деятельности в подразделениях организационной системы;
- виды деятельности организационной системы;
- деятельность организационной системы в целом.

Техническим результатом является расширение функциональных возможностей за счёт возможностей по предотвращению угроз отдельным

видам деятельности и деятельности в целом организационной системы и по сокращению времени разрешения проблемных ситуаций, если угрозы возникли.

Способ поддержки деятельности организационной системы [7], помимо применения в приведённой выше системе управления деятельностью организационных систем [4], лежит в основе следующих инновационных разработок:

- системы ситуационно-аналитических центров организационной системы [8];
- центра управления организационной системы [9];
- центра мониторинга устойчивости информационных систем [10];
- центра поддержки устойчивости информационных систем [11].

Общее, что объединяет данные технические решения, это целевые установки на их разработку – достижение максимальной степени автоматизации процессов управления на основе подготовки и применения априорных и ретроспективных сценариев для автоматического их исполнения робототехническими объектами, информационными системами или для принятия решений субъектами управления в организационных системах в зависимости от имеющихся ресурсов и сложившихся обстоятельств в среде деятельности.

Система ситуационно-аналитических центров организационной системы

Техническое решение – система ситуационно-аналитических центров организационной системы [8] относится к области управления деятельностью организационных систем, предметной областью являются системы подготовки и исполнения решений.

Системы ситуационных и аналитических центров организационных систем являются концентрацией современных информационных технологий, предназначенных для автоматизированной поддержки при управлении деятельностью организационных систем, в целом – министерств и ведомств, корпораций, предприятий, банков, и, в частности, при управлении видами деятельности подразделений организационных систем, размещённых как в стационарных, так и в мобильных объектах. Преимуществом настоящего технического решения [8] перед его аналогами – техническими решениями [5, 13], является обеспечение возможности для автоматизированной поддержки деятельности организационной системы при одновременной выработке планов разрешения нескольких проблемных ситуаций, относящихся к различным видам деятельности её подразделений, и/или плана разрешения ряда проблемных ситуаций, порождённых одной проблемой, с разными степенями влияния на виды деятельности подразделений организационной системы.

Задачей, на решение которой была направлена разработка технического решения, является предложение новой и улучшенной системы ситуационно-аналитических центров организационной системы, способной сократить сроки разрешения сложных проблемных ситуаций.

На рис. 15 приведена структурная схема системы ситуационно-аналитических центров организационной системы [8].

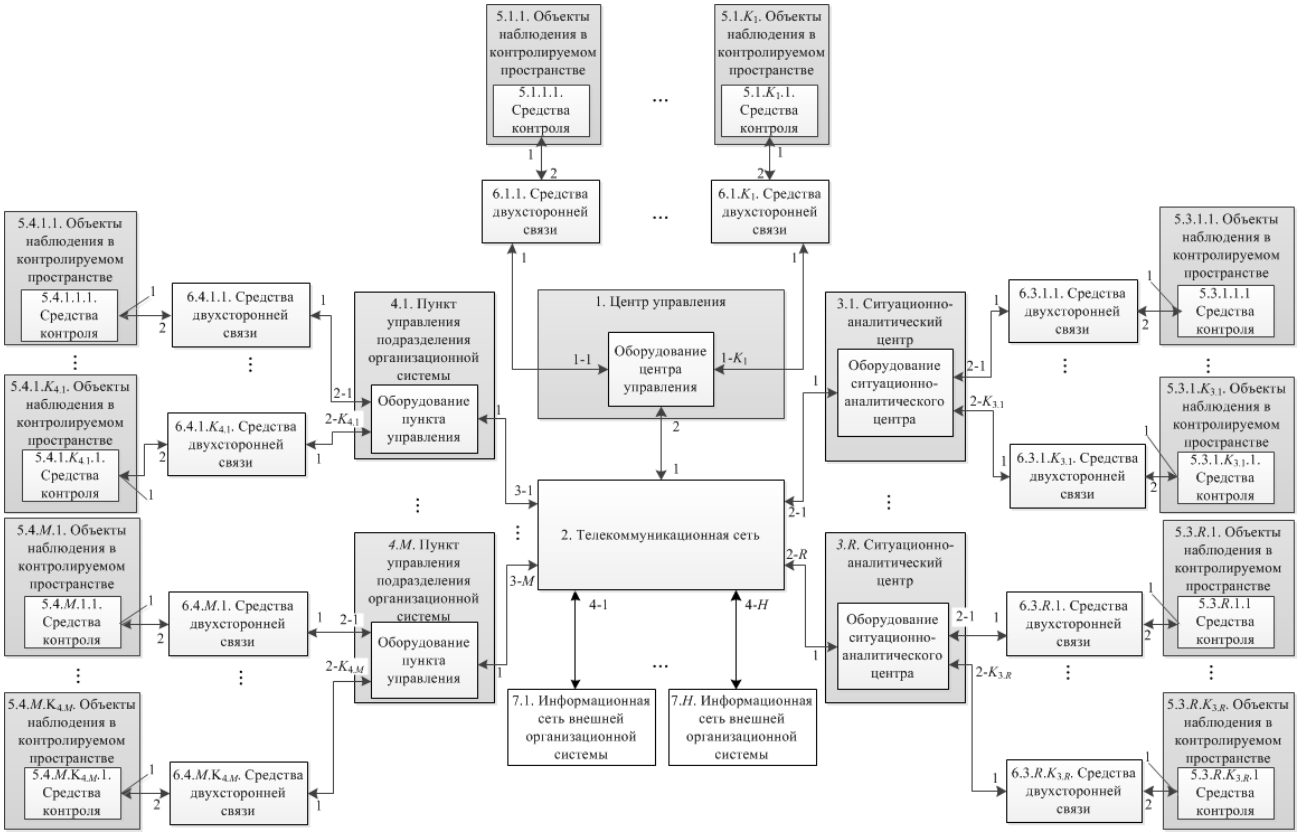


Рис. 15. Структура системы ситуационно-аналитических центров организационной системы

Система ситуационно-аналитических центров организационной системы (рис. 15) работает следующим образом.

В исходном состоянии в вычислительных комплексах центра управления (ЦУ), ситуационно-аналитических центров (САЦ) и пунктов управления (ПУ) формируются и запоминаются технологические данные. Перечень данных может быть аналогичен перечню данных, приведённых выше в описании системы управления деятельностью организационных систем [4].

На стадии эксплуатации системы средства контроля над объектами наблюдения в контролируемом пространстве производят сбор данных о состоянии этих объектов, осуществляется передача этих данных с помощью средств двухсторонней связи и интерфейсов оборудования в ЦУ, САЦ и ПУ, в том числе:

- передачу данных с видеоизображениями объектов наблюдения на мониторы компьютеров, объединённых в компьютерные сети, и на экраны мультимедиа в рабочих залах ЦУ, САЦ и ПУ;
- передачу данных о фактических показателях наблюдаемых объектов, представленных безразмерными числами и/или единицами измерений, в вычислительные комплексы ЦУ, САЦ и ПУ.

В вычислительных комплексах ЦУ, САЦ и ПУ в соответствии с зонами

их ответственности производится обработка данных о фактических и требуемых показателях объектов наблюдения в контролируемом пространстве и выработка данных о фактических состояниях деятельности организационной системы в целом, видах деятельности и о состоянии объектов наблюдения. В зависимости от результатов обработки данных вырабатываются следующие сценарии:

- по устранению угрозы для деятельности организационной системы в целом, для отдельных видов деятельности организационной системы и для деятельности подразделений организационной системы;
- по предотвращению угрозы для деятельности организационной системы в целом, для отдельных видов деятельности организационной системы и для деятельности подразделений организационной системы;
- по повышению эффективности деятельности организационной системы в целом, отдельных видов деятельности организационной системы и деятельности подразделений организационной системы;

В состав данных о сценариях входят: данные об объектах наблюдения в контролируемом пространстве, с которыми должны быть проведены необходимые действия; данные о силах и средствах, которые требуется привлечь для проведения этих действий; данные о порядке проведения действий. И другие данные, которые необходимы для выполнения действий по устранению угроз различного характера, по их предотвращению или по выполнению плановых работ, направленных на повышение эффективности осуществляемой деятельности, включая данные об адресатах подразделений организационной системы и внешних организационных систем, привлекаемых к работам.

Данные о сценариях и, при необходимости, данные с видеоизображениями объектов наблюдения в контролируемом пространстве передаются с помощью интерфейсов оборудования ЦУ, САЦ и ПУ и с помощью телекоммуникационной сети в зависимости от назначения:

- в компьютеры, объединённые в компьютерные сети в рабочих залах ЦУ, САЦ и ПУ;
- в видеосистемы и в компьютер настройки видеосистемы ситуационных комнат ЦУ и САЦ, при этом компьютер настройки обеспечивает распределение поверхности экрана на отдельные сегменты с параметрами измерения, в зависимости от числа и приоритетов, размещаемых на поверхности данных;
- на экраны мультимедиа в рабочих залах ЦУ, САЦ и ПУ.

При этом различают данные по следующим категориям: критические, предупреждающие и плановые данные о сценариях, предназначенные для подготовки и исполнения решений соответственно по устранению угроз, их предотвращению и по выполнению плановых работ в среде деятельности организационной системы в целом, видов деятельности и видов деятельности, осуществляемой в её подразделениях. На рис. 16 – рис. 18 приведены диаграммы, иллюстрирующие вариант распределения данных о сценариях

различной категории ($W_{крит.}$, $W_{пред.}$ и др.) на оси эффективности деятельности организационной системы для ЦУ, САЦ и ПУ по интервалам, определяемым критическими и допустимыми показателями эффективности деятельности ($\Delta D_{крит.}$, $\Delta D_{доп.}$ и др.).

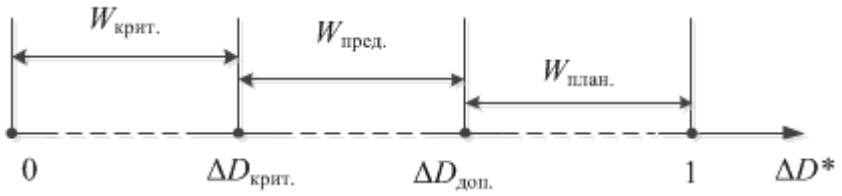


Рис. 16. Соотношения сценариев и показателей эффективности для ЦУ

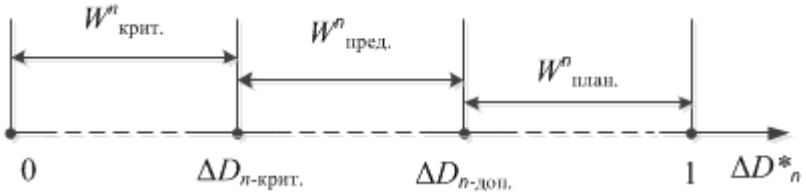


Рис. 17. Соотношения сценариев и показателей эффективности для САЦ

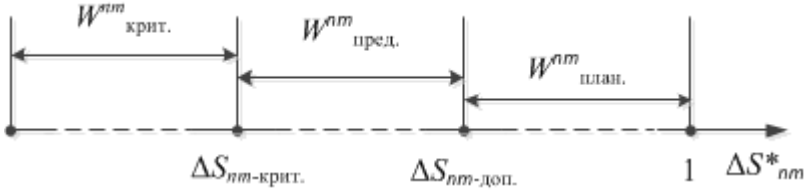


Рис. 18. Соотношения сценариев и показателей эффективности для ПУ

Основным техническим результатом применения технического решения – системы ситуационно-аналитических центров организационной системы, является повышение эффективности процессов принятия и исполнения решений за счёт автоматизированной выработки сценариев подготовки и исполнения управляющих решений по ликвидации проблемных ситуаций.

На рис. 19 представлен пример алгоритма функционирования системы ситуационно-аналитических центров при управлении разрешением проблемы в зоне ответственности САЦ или ЦУ.

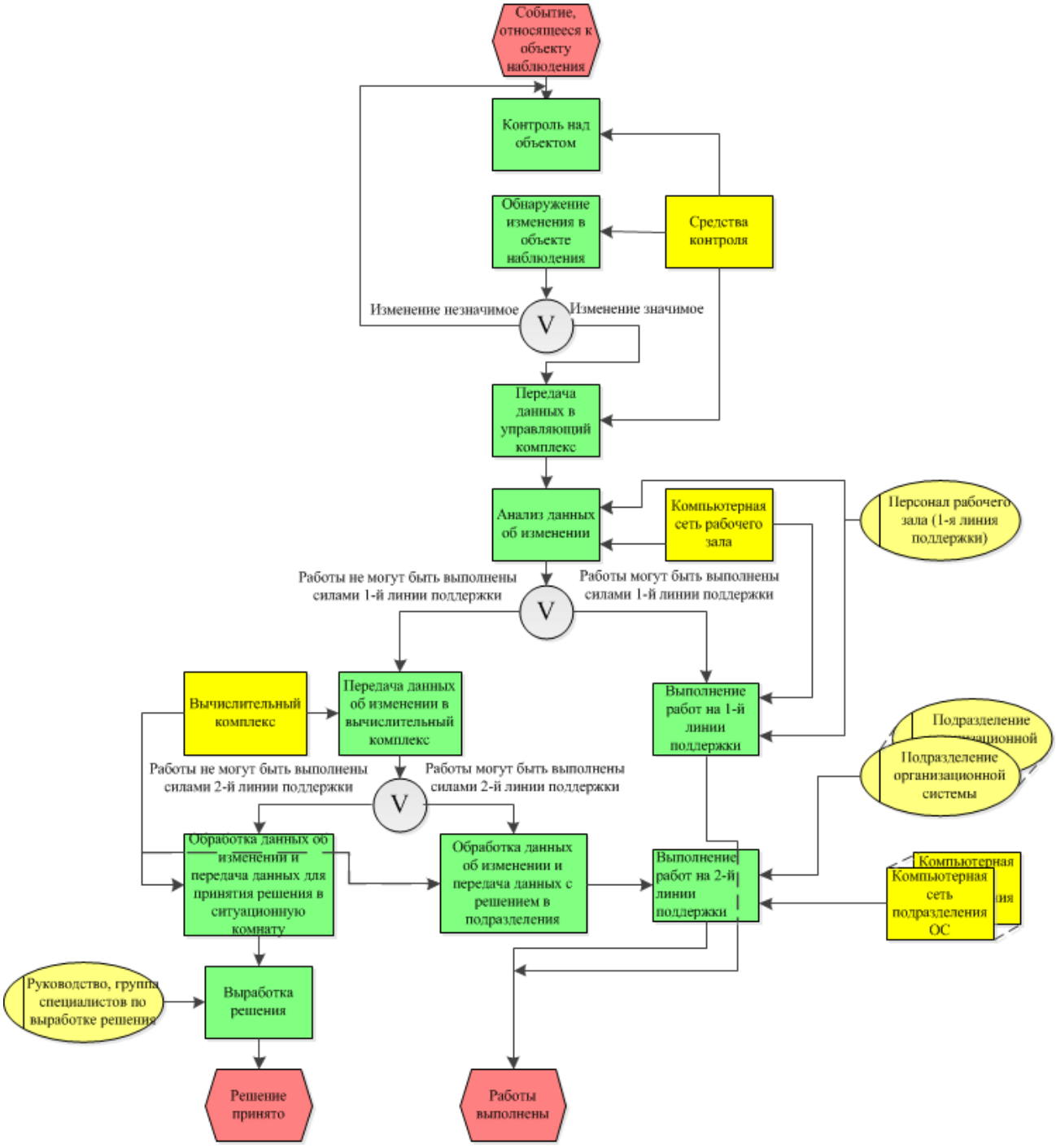


Рис. 19. Алгоритм работы системы при управлении разрешением проблемы в контролируемой зоне (пример)

Центр управления организационной системы

Техническое решение – центр управления организационной системы [9] относится к области управления деятельностью организационных систем, предметной областью являются системы подготовки и исполнения решений.

Отличительной чертой настоящего технического решения от системы ситуационно-аналитических центров организационной системы [8], рассмотренной выше, является централизованное выполнение всех этапов способа поддержки деятельности организационной системы [7] в одном месте – центре управления организационной системы, в то время, как в системе

ситуационно-аналитических центров ответственность за выполнение действий этапов данного способа распределена между ЦУ, САЦ и ПУ (рис. 15).

На рис. 20 приведена структурна схема центра управления организационной системы [9].

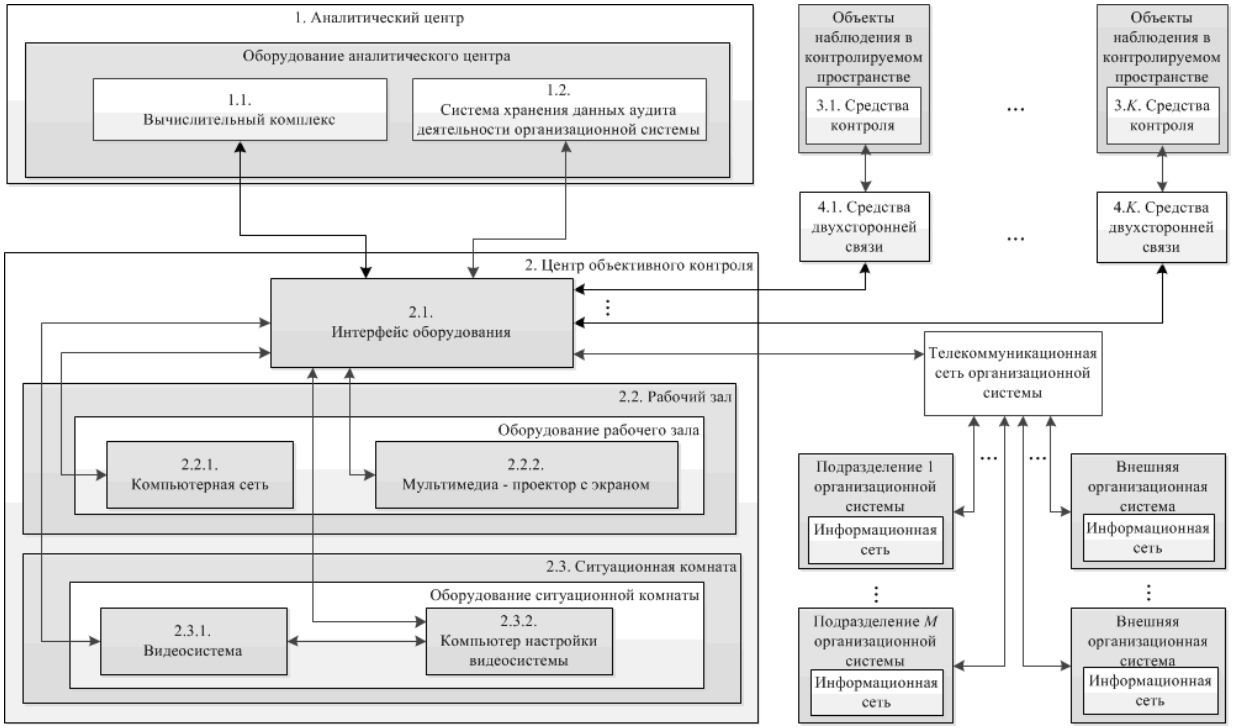


Рис. 20. Структура центра управления организационной системы

Центр управления организационной системы (ЦУ ОС) (рис. 20) работает следующим образом.

В исходном состоянии в вычислительном комплексе ЦУ ОС формируются и запоминаются технологические данные. Перечень данных может быть аналогичен перечню данных, приведённых выше в описании системы управления деятельностью организационных систем [4].

На стадии эксплуатации ЦУ ОС средства контроля над объектами наблюдения в контролируемом пространстве производят сбор данных о состоянии этих объектов, осуществляется передача этих данных с помощью средств двухсторонней связи и интерфейсов оборудования в ЦУ ОС, в том числе:

- передачу данных с видеоизображениями объектов наблюдения на мониторы компьютеров, объединённых в компьютерную сеть, и на экраны мультимедиа в рабочем зале;
- передачу данных о фактических показателях наблюдаемых объектов, представленных безразмерными числами и/или единицами измерений, в вычислительный комплекс.

В вычислительном комплексе ЦУ ОС производится обработка данных о фактических и требуемых показателях объектов наблюдения в контролируемом пространстве и выработка данных о фактических состояниях деятельности организационной системы в целом, видах деятельности и о состоянии объектов

наблюдения. Алгоритмы обработки данных могут быть аналогичными алгоритмам обработки данных, выполняемым рассмотренной выше системой ситуационно-аналитических центров организационной системы [8].

Центр мониторинга устойчивости информационных систем

Техническое решение – центр мониторинга устойчивости информационных систем (ЦМУ ИС) [10], относится к области управления деятельностью организационных систем – предприятий и их подразделений информатизации, предметной областью являются системы подготовки решений по предотвращению и ликвидации проблем в среде деятельности этих организационных систем.

Техническим результатом является расширение функциональных возможностей за счёт возможности формирования, сохранения, отображения и передачи данных об устойчивости информационных систем субъектам управления деятельностью организационных систем.

Функционирование информационных систем, предназначенных для автоматизации управления в подразделениях и в организационной системе, происходит в постоянном взаимодействии средств информационных систем между собой и с внешней средой. При этом широкий класс такого взаимодействия представляет собой разнообразные конфликты, существенно влияющие на достижение целей деятельности организационной системы в целом, или её подразделений. Эти конфликты приводят к разрушению информационных ресурсов, нарушению штатных информационных процессов, и, как следствие, срыву выполнения системных и прикладных функций собственно подразделений или в целом предприятия. Все это предопределяет наличие механизмов, которые должны обеспечивать такое качество информационных систем, как способность сохранения и/или восстановления функций в условиях различного рода неблагоприятных воздействий. Данное качество назовём здесь *устойчивостью* (функциональной устойчивостью) информационных систем. В общем случае показатели устойчивости являются интегральными и, как правило, включают в себя показатели надежности, живучести и безопасности. В ряде случаев показатели устойчивости или ограничиваются, в частности, показателями устойчивости трактов или в целом информационных систем, или, наоборот расширяются – дополнительно вводятся показатели своевременности предоставления информации [13].

Общим свойством настоящего технического решения и технических решений, рассмотренных выше, является выполнение этапов способа поддержки деятельности организационной системы [7], относящихся к формированию технологических данных, анализу эффективности видов деятельности организационных систем (конкретно для ЦМУ ИС – деятельности по информационной поддержке бизнес процессов) и предоставление результатов анализа субъектам управления.

На рис. 21 приведена структурная схема центра мониторинга устойчивости информационных систем [10].

Рис. 21. Структура центра мониторинга устойчивости информационных систем

При подготовке ЦМУ ИС к работе формируются и передаются в соответствующие компоненты ЦМУ ИС команды управления коммутацией, технологические данные – о составе средств в информационных системах, для администрирования и настройки этих компонентов, о составе средств в трактах информационных систем.

ЦМУ ИС работает следующим образом (рис. 21).

На первый вход 5 ЦМУ ИС и далее в маршрутизатор 1 поступают данные от датчиков контроля состояний средств информационных систем. К этим средствам относятся – вычислительные средства (серверы, персональные компьютеры и др.), телекоммуникационные средства (коммутаторы пакетов, сообщений или каналов, маршрутизаторы, устройства защиты и др.), инженерные средства, здания и помещения, средства жизнеобеспечения субъектов – пользователей информационных систем, программные средства и другие средства, оказывающие влияние на устойчивость информационных систем. Данные содержат следующую информацию о средстве:

– данные – индивидуальный идентификатор средства;
– данные – код состояния средства.

Коды состояний средств, в зависимости от типа источников информации – датчиков, могут быть составными, включающими в себя коды, характеризующие различные свойства средства. Например – надёжность, живучесть (способность выполнять заданные функции при различных внешних негативных воздействиях), безопасность (защищённость от опасных

программно-технических воздействий), своевременность (время передачи или обработки средством информации). В общем случае коды состояния характеризуют средство как «средство работоспособно» или «средство неработоспособно».

Маршрутизатор 1 на основании принятых данных об индивидуальном идентификаторе средства и с помощью данных о составе средств в информационных системах определяет индивидуальные идентификаторы информационных систем, функционирование которых обеспечивается данным средством. По образованному маршрутизатором 1 тракту индивидуальные идентификаторы информационных систем и данные, принятые от датчиков, поступают в комплекс 2 сбора информации.

В комплексе 2 сбора информации каждый раз, когда поступают новые данные от датчиков, они запоминаются, производится их сравнение с данными о состоянии соответствующих средств, которые поступили ранее. Различие в данных означает изменение состояния соответствующего средства. В этом случае новые данные об этом средстве запоминаются в комплексе 2 и передаются:

- с первого выхода комплекса 2 на первый выход 9 ЦМУ ИС, при этом пунктом назначением этого действия может быть компьютерная сеть подразделения технической поддержки организационной системы или другой пункт, в зависимости от области применения ЦМУ ИС;
- со второго выхода комплекса 2 в комплекс 3 определения устойчивости информационных систем.

Комплекс 3 определения устойчивости информационных систем на основании данных об индивидуальном идентификаторе средства, о коде состояния средства, об индивидуальных идентификаторах информационных систем, функционирование которых обеспечивается данным средством, и с помощью сохранённых в комплексе 3 данных о составе средств в трактах информационных систем вырабатывает данные об устойчивости информационных систем. Выработка этих данных производится исходя из представления об устойчивости, которое приведено выше. Затем эти данные передаются в комплекс 2 сбора информации, который с помощью данных о составе средств в информационных системах сохраняет поступившие из комплекса 3 данные об устойчивости информационных систем и осуществляет передачу новых данных об устойчивости информационных систем со своего третьего выхода:

- на второй выход 10 ЦМУ ИС, при этом пунктом назначения этого действия может быть компьютерная сеть подразделения технической поддержки организационной системы или другой пункт, в зависимости от области применения ЦМУ ИС;
- на четвёртый вход маршрутизатора 1.

В маршрутизаторе 1 принятые данные об устойчивости информационных систем передаются по заранее подготовленному тракту на первый вход комплекса 4 отображения информации.

Комплекс 4 отображения информации осуществляет вывод поступивших

данных об устойчивости информационных систем на экраны для их отображения субъектам управления организационной системы. В зависимости от данных настройки комплекса 4 (настроечные данные поступили ранее на его второй вход со второго входа 6 ЦМУ ИС) и от состава оборудования комплекса 4, данные об устойчивости информационных систем могут поступить на мониторы из состава оборудования рабочих мест субъектов управления и/или на коллективный экран (экраны). При этом отображение информации, содержащейся в поступивших данных, представляется в виде диаграмм, графиков или в другом виде, в соответствии с применяемыми в комплексе 4 прикладными программами и действиями, выполняемыми субъектами управления.

Наиболее востребованной областью применения настоящего технического решения являются организационные системы, выполняющие свою деятельность в условиях ожидаемых и существующих угроз техногенного, природного или человеческого характера. В таких организационных системах требуется постоянный контроль над устойчивостью информационных систем, с целью получения своевременной и достоверной информации. При этом существует непосредственная связь между показателями своевременности и достоверности информации, с одной стороны, и показателями устойчивости информационных систем и надёжности технических средств, обеспечивающих их функционирование, с другой стороны. В работах [13–15] показана и обоснована эта зависимость.

Центр поддержки устойчивости информационных систем

Техническое решение – центр поддержки устойчивости информационных систем (ЦПУ ИС) [11], относится к области управления деятельностью подразделений информатизации, предметной областью являются системы подготовки и исполнения решений по предотвращению и ликвидации проблем в среде деятельности этих подразделений.

Разработка данного технического решения была обусловлена функциональной недостаточностью ЦМУ ИС [10] в связи с отсутствием возможности автоматического определения в среде функционирования информационных систем проблем – причин неработоспособности технических средств; ошибок в программах, неправильных действий пользователей и персонала. Фиксируются факты проявления проблем – неработоспособные состояния контролируемых объектов – инциденты. Проблемы же определяются «вручную» или автоматизированным способом с помощью специализированных программ, но уже после проявления этих проблем.

Продолжительность состояний неработоспособности информационных систем определяет уровень их устойчивости и, следовательно, уровень непрерывности автоматизируемых с помощью этих систем видов деятельности организационных систем – ведомств, учреждений и предприятий. Чем продолжительнее время определения проблемы, тем больше число инцидентов, порождённых этой проблемой, и тем ниже уровень устойчивости. Таким образом, технические решения, которые обеспечивают сокращение времени

определения проблем, тем самым обеспечивают повышение устойчивости ИС и, в конечном счёте, повышение эффективности деятельности организационных систем. К таким техническим решениям относится настоящее техническое решение – ЦПУ ИС [11], которое обеспечивает автоматическое определение проблем.

ЦПУ ИС выполнен с возможностью на основе обработки данных, поступающих с входов для приёма данных от датчиков контроля, данных о составе средств информационных систем, данных о составе средств в трактах информационных систем и данных о моделях исследований автоматически формировать, сохранять, отображать и передавать по назначению данные о проблемах в среде функционирования информационных систем, в том числе данные о неисправности технических средств и об ошибках в программах.

На рис. 22 приведена структурная схема центра поддержки устойчивости информационных систем [11].

Рис. 22. Структура центра поддержки устойчивости информационных систем

При подготовке ЦПУ ИС к работе формируются и передаются в соответствующие компоненты ЦПУ ИС, помимо таких же команд управления и данных, как в ЦМУ ИС [10], данные о моделях исследований. Эти данные используются при функционировании комплекса 5 системных исследований для определения проблем в информационных системах, относящихся к различным категориям, в том числе к проблемам, обусловленным

неисправностями технических средств, ошибками в программах, несоблюдением заданных уровней ИТ-услуг.

ЦПУ ИС в части мониторинга устойчивости информационных систем работает аналогично работе ЦМУ ИС, при этом вырабатываются данные о матрице текущих состояниях средств и трактов информационных систем.

Комплекс 5 системных исследований (рис. 22), каждый раз после приёма данных о матрице текущих состояний средств и трактов информационных систем запоминает эти данные и производит действия по определению проблемы в информационных системах. Исходными данными, помимо данных матриц, являются данные о показателях средств, поступившие из комплекса 2 и данные о моделях исследований, хранящиеся в комплексе 5.

Рассмотрим примеры работы ЦПУ ИС по определению проблем.

Пример 1. Модель исследования при определении неисправности технического средства:

- после приёма данных об очередной матрице текущих состояний средств и трактов информационных систем для каждого технического средства, указанного в матрице, определяется число $n(S)$ неработоспособных состояний технического средства S, с учётом данных, полученных в предыдущих матрицах;
- если $n(S)$ равно заданному числу $n_{зад.}(S)$, то определяются числа $n(S_k)$ одинаковых показателей для этого средства, которые относятся к каждому из $n_{зад.}(S)$ случаев неработоспособности, где k – число показателей средства;
- если для любого показателя i из совокупности k показателей число $n(S_i)$ равно заданному числу $n_{зад.}(S_i)$ и сумма таких показателей равно заданному числу $n_{зад.}(S_k)$, то формируются данные о существовании проблемы, обусловленной техническим средством S, в состав этих данных входят блоки данных об идентификаторе средства, информационных системах и их трактах, функционирование которых обеспечивает данное средство;
- сформированные данные передаются, например, в центр технической поддержки организационной системы для решения проблемы или в другой пункт, в соответствии с регламентом.

Пример 2. Модель исследования при определении ошибки в программе аналогична модели, рассмотренной в 1-м примере, и дополнительно определяется число сбоев (остановки работы) каждого экземпляра программы от одного и того же производителя, одной и той же марки, независимо от места использования экземпляра программы в трактах и в информационных системах.

Физическая трактовка приведённых выше моделей исследования заключается в том, что автоматически определяется проблема, которая была причиной инцидентов в предыдущих $n_{зад.}(S)$-1 случаях неработоспособности средства S. Для восстановления работоспособности средства S в указанных случаях применялись обходные способы, которые не затрагивали корневую причину неисправности – проблему. Определение проблемы позволяет

максимально быстро начать работы по её решению и устранению корневой причины неисправности технического средства.

Заключение

Инновационность представленных в статье технических решений заключается в создании, расширении и применении базы знаний сценариев управленческих решений на основе:

- априорного метода – путём обработки и анализа ретроспективной информации о всех сущностях, оказавших влияние на состояние деятельности организационных систем в предшествующие интервалы времени;
- опытного добавления знаний путём обработки вновь созданного сценария и уже применённого к конкретной обстановке в среде деятельности и анализа всех обстоятельств, относящихся к этой обстановке;
- проверки актуальности компонентов выбранного из базы знаний сценария решения непосредственно до предоставления его лицу, принимающему решение или до передачи его на исполнение, и, при необходимости, модернизации этого сценария.

Положительный эффект от внедрения представленных в статье изобретений и полезных моделей заключается:

- в повышении устойчивости государственного, ведомственного и других видов управления;
- в повышении достоверности сценариев управленческих решений и, как следствие, в сокращении сроков достижения целей управления при предотвращении угроз для деятельности организационных систем различных уровней иерархии, при минимизации негативных последствий от уже реализованных угроз и при выполнении плановых работ;
- в повышении устойчивости функционирования информационных систем в организационных системах;
- в повышение устойчивости бизнеса предприятий различных отраслей хозяйствования.

Применение представленных в статье технических решений в проектах, ведущихся в области управления организационными системами, позволит непрерывно отслеживать состояние деятельности и сократить время на принятие и исполнение управляющих решений в ведомствах, на предприятиях и в учреждениях.

Литература

1. О стратегии национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 // Официальный интернет-портал правовой информации [Электронный ресурс]. – URL: http://publication.pravo.gov.ru/Document/View/0001201512310038 (дата обращения 11.09.2016).

2. Зацаринный А. А., Козлов С. В., Шабанов А. П. Об информационной поддержке деятельности в системах управления критическими технологиями на основе ситуационных центров // Системы управления, связи и безопасности 2015. № 4. С. 98-113. – URL: http://sccs.intelgr.com/archive/2015-04/05-Zatsarinnyy.pdf (дата обращения 11.09.2016).

3. Шабанов А. П. Инновации: от устройств обмена информацией до интегрированных систем управления. Часть 1 – Устройства обмена информацией // Системы управления, связи и безопасности. 2016. № 2. С. 1-43. URL: http://sccs.intelgr.com/archive/2016-02/01-Shabanov.pdf (дата обращения 11.09.2016).

4. Зацаринный А. А., Шабанов А. П. Система управления деятельностью организационных систем // Патент на изобретение RU 2595335 C2, опубл. 27.08.2016, бюл. № 24. – URL: http://elibrary.ru/item.asp?id=26545435 (дата обращения 11.09.2016).

5. Финк Ю. М., Коваленко В. Н. Система объективного контроля ситуации // Патент на полезную модель RU 28927 U1, опубл. 20.04.2003, бюл. № 11.

6. Скварник С. В., Котов С. Ю., Орлянский В. Н., Кучинский С. В. Система информационно-технического взаимодействия центра управления и периферийных средств обслуживания воздушного движения // Патент на полезную модель RU 118092 U1, опубл. 10.07.2012, бюл. № 19.

7. Зацаринный А. А., Сучков А. П., Шабанов А. П. Способ поддержки деятельности организационной системы // Патент на изобретение RU 2532723 C2, опубл. 10.11.2014, бюл. № 31. – URL: http://elibrary.ru/item.asp?id=25995754 (дата обращения 11.09.2016).

8. Зацаринный А. А., Козлов С. В., Сучков А. П., Шабанов А. П. Система ситуационно-аналитических центров организационной системы // Патент на изобретение RU 2533090 C1, опубл. 20.11.2014, бюл. № 32. – URL: http://elibrary.ru/item.asp?id=25995572 (дата обращения 11.09.2016).

9. Зацаринный А. А., Козлов С. В., Сучков А. П., Шабанов А. П. Центр управления организационной системы // Патент на полезную модель RU 127493 U1, опубл. 27.04.2013, бюл. № 12. – URL: http://elibrary.ru/item.asp?id=25995467 (дата обращения 12.09.2016).

10. Голяндин А. Н., Шабанов А. П. Центр мониторинга устойчивости информационных систем // Патент на полезную модель RU 130109 U1, опубл. 10.07.2013, бюл. № 19. – URL: http://elibrary.ru/item.asp?id=26073985 (дата обращения 12.09.2016).

11. Голяндин А. Н., Шабанов А. П. Центр поддержки устойчивости информационных систем // Патент на полезную модель RU 132227 U1, опубл. 10.09.2013, бюл. № 25. – URL: http://elibrary.ru/item.asp?id=25998536 (дата обращения 12.09.2016).

12. Гольдштейн С. К., Кудрявцев А. Г. Ситуационный центр // Патент на полезную модель RU 105031 U1, опубл. 27.05.2011, бюл. № 11.

13. Зацаринный А. А., Шабанов А. П. Ситуационные центры: информация - процессы – организация // Электросвязь. 2011. № 6. С. 42-46. – URL: http://elibrary.ru/item.asp?id=16540829 (дата обращения 12.09.2016).

14. Шабанов А. П. Исследование граничных условий стабильности информационных систем // Бизнес-Информатика. 2010. № 2 (12). С. 24-36. – URL: http://elibrary.ru/item.asp?id=15113138 (дата обращения 12.09.2016).

15. Зацаринный А. А., Шабанов А.П. Методологический подход к управлению качеством информации в сложных инфокоммуникационных проектах // Системы и средства информатики. 2011. № 2. С. 2-19. – URL: http://elibrary.ru/item.asp?id=17104158 (дата обращения 12.09.2016).

References

1. The strategy of national security of the Russian Federation. Decree of the President of the Russian Federation from December 31, 2015, no. 683. *Ofitsial'nyi internet-portal pravovoi informatsii* [Online Resource]. Available at: http://publication.pravo.gov.ru/Document/View/0001201512310038 (accessed 15 November 2014) (in Russian).

2. Zatsarinnyy A. A., Kozlov S. V., Shabanov A. P. Information Support for the Activities of the Critical Technologies in Control Systems Based on Situational Centers. *Systems of Control, Communication and Security*, 2015, no. 4, pp. 98-113. Available at: http://sccs.intelgr.com/archive/2015-04/05-Zatsarinnyy.pdf (accessed 27 March 2016) (in Russian).

3. Shabanov A. P. Innovation: Sharing Devices to Integrated Management Systems. Part 1 – Sharing Devices. *Systems of Control, Communication and Security*, 2016, no. 2, pp. 1-43. Available at: http://sccs.intelgr.com/archive/2016-02/01-Shabanov.pdf (accessed 12 September 2016) (in Russian).

4. Zatsarinnyy A. A., Shabanov A. P. Organizational systems management system. Patent Russia, no. RU 2595335 C2. Publish. 27.08.2016, bul. no. 24 (in Russian).

5. Fink U. M., Kovalenko V. N. System of the objective control of the situation. Patent Russia, no. RU 28927 U1. Publish. 20.04.2003, bul. no. 11 (in Russian).

6. Skvarnik S. V., Kotov S. U., Orljansky V. N., Kuchinsky S. V. Information technology system control center and peripheral interaction means air traffic services. Patent Russia, no. RU 118092 U1. Publish. 10.07.2012, bul. no. 19 (in Russian).

7. Zatsarinnyy A. A., Suchkov A. P., Shabanov A. P. Method of supporting operation of organizational system. Patent Russia, no. RU 2532723 C2. Publish. 10.11.2014, bul. no. 31 (in Russian).

8. Zatsarinnyy A. A., Kozlov S. V., Suchkov A. P., Shabanov A. P. System for situation-analytical centers of organizational system. Patent Russia, no. RU 2533090 C2. Publish. 20.11.2014, bul. no. 32 (in Russian).

9. Zatsarinnyy A. A., Kozlov S. V., Suchkov A. P., Shabanov A. P. Management Center of organizational system. Patent Russia, no. RU 127493 U1. Publish. 27.04.2013, bul. no. 12 (in Russian).

10. Goljandin A. N., Shabanov A. P. Monitoring Center for sustainability information systems. Patent Russia, no. RU 130109 U1. Publish. 10.07.2013, bul. no. 19 (in Russian).

11. Goljandin A. N., Shabanov A. P. Stability of information systems support center. Patent Russia, no. RU 132227 U1. Publish. 10.09.2013, bul. no. 25 (in Russian).

12. Goldshtejn S. K., Kudrjavtsev A. G. The situation center. Patent Russia, no. RU 105031 U1. Publish. 27.05.2011, bul. no. 11 (in Russian).

13. Zatsarinnyy A. A., Shabanov A. P. Situational Centers: information – processes – organization. *Telecommunications*, 2011, no. 6, pp. 42-46. Available at: http://elibrary.ru/item.asp?id=16540829 (accessed 12 September 2016) (in Russian).

14. Shabanov A. P. The study of conditions of stability information system. *Business Informatics*, 2010, vol. 12, no. 2, pp. 24-36. Available at: http://elibrary.ru/item.asp?id=15113138 (accessed 12 September 2016) (in Russian).

15. Zatsarinnyy A. A., Shabanov A. P. Methodological approach to quality management of information in complex infocommunication projects // *Systems and informatics tools*, 2011, Issue 21, no. 2, pp. 2-19. Available at: http://elibrary.ru/item.asp?id=17104158 (accessed 12 September 2016) (in Russian).

Статья поступила 13 сентября 2016 г.

Информация об авторе

Шабанов Александр Петрович – доктор технических наук. Ведущий научный сотрудник. Институт проблем информатики Федерального исследовательского центра «Информатика и управление» РАН. Область научных интересов: информационная поддержка деятельности организационных систем – ведомств, предприятий, учреждений. E-mail: apshabanov@mail.ru

Адрес: Россия, 119333, Москва, ул. Вавилова, д. 44, кор. 2.

Innovation: Sharing Devices to Integrated Management Systems Part 2 – Management of Organizational Systems

A. P. Shabanov

Introduction. *About the inventions that relate to critical technologies - technology information and control systems, that define the main directions of scientific and technological development.* ***Characteristic.*** *Analysis of technical decisions has been implemented in two time periods of modern history of the domestic electronics industry – during the formation of integration of scientific-industrial complexes and large-scale system projects in 1980-ies, and during recovery of this approach in 2010-ies. In the first stage of technical solutions have been developed for the collection and processing of relevant information about facilities management, to improve the sustainability of tracts of computer networks using radio communications and fiber-optic connection, on time management providing information and other. In the second period, these technical solutions have provided the basis for the development of innovative ways of information support for the activities of organizational systems – departments, enterprises and institutions, for the development of integration of control systems of the activities of organizational systems, which consolidated to solve*

common tasks. ***Technical result.*** *The technical solutions, which are developed in the first period, improves qualitative indicators of control systems in timeliness and reliability. The technical solutions, which are developed in the second period, helps to ensure the maximum degree of automation based on prior training scenarios for the adoption and implementation of the control solutions.* ***The essence.*** *Common property that unites all inventions is the author's approach to finding inventive concept and its development. This approach includes the famous stages and phases of formation, accumulation and use of knowledge about entities, that affect the field of activity, for which created the invention This knowledge is carried out by processing the data in computer systems and components in the components of computer networks with exposure on the order data and their contents.* ***Practical significance.*** *Information on inventions developed in the first period was published in the previous issue of the magazine in order to use the ideas that underlie inventions for their implementation based on modern computing tools. Information on inventions developed in the second period, relating to the management of organizational systems, is published in order to extend the potential of their introduction into the control systems of organizational systems.*

Key words: *inventions, critical technologies, control systems, information systems, communication systems, accumulation of knowledge, solution scripts.*

Information about Author

Alexander Petrovich Shabanov – Dr. habil. of Engineering Sciences. Leading Researcher. Institute of Informatics problem of FRC CSM RAS. Field of research: information support for the activities of the organizational systems – departments, enterprises and institutions. E–mail: apshabanov@mail.ru

Address: Russia, 119333, Moscow, Vavilova str., h. 44, s. 2.

УДК 004.021

Расширенное микширование аудиопотоков для многопроцессорных устройств в телекоммуникациях

Колпаков А. А., Кропотов Ю. А., Белов А. А., Холкина Н. Е.

Постановка задачи: *В работе рассмотрены вопросы расширенного микширования аудиопотоков для их обработки на графических процессорах, в которых комбинируются множество потоков путем использования двухпроходного рендера, что существенно снижает время переключения между буферами. Методом экспериментальных компьютерных сравнительных исследований было осуществлено оценивание производительности разработанного алгоритма.* ***Целью работы*** *является разработка эффективного алгоритма микширования аудиопотоков для обработки на графических процессорах.* ***Новизна:*** *элементами новизны представленного алгоритма является использование в его составе двухпроходного рендера.* ***Используемые методы:*** *метод переноса операций вычислений на графические процессоры с применением шейдерных программ.* ***Результат:*** *результаты исследований показали, что применение разработанного алгоритма приводит к существенному увеличению производительности вычислений.* ***Практическая значимость****: представленное решение предполагается реализовать в виде программного обеспечения многопроцессорных устройств в системах телекоммуникаций.*

Ключевые слова: *двухпроходной рендер, алгоритм повышения производительности, параллельные вычисления, гетерогенные вычислительные системы, графические процессоры, микширование аудио данных.*

Введение

С развитием современных компьютерных сетей такие мультимедиа Internet-приложения, как удаленная работа по сети, совместные разработки и видео конференции, прочно вошли в повседневную жизнь. Согласно исследованиям [1] 75% межпользовательского общения по сети приходится на голосовой трафик. Поскольку голосовое общение играет такую важную роль, нельзя исключать и голосовые конференции с несколькими участниками.

Простейший сценарий организации голосовой коммуникации заключается в том, что каждый источник звука шлет свой аудиопоток каждому приемнику независимо. Такой метод прост и удобен, но требует высокой пропускной способности сети, что не всегда можно обеспечить. Поэтому лучшим методом может служить микширование аудио, что означает комбинирование аудиопотоков от каждого источника в один. Исходя из возможности звуковых волн накладываться друг на друга, данный метод может обеспечивать приемлемое качество звука, при этом обеспечивая снижение загруженности сети. Однако, применение данного метода может существенно увеличить нагрузку на центральный процессор сервера, что может негативно сказываться на производительность системы в целом. Выходом из данной ситуации может стать применение графических процессоров для решения данной задачи.

Проблемы использования графических процессоров для аудио микширования

Хотя графические процессоры достаточно производительны, существует несколько проблем в использовании их для аудио микширования, которые связаны с архитектурой и ограниченностью функционала [2].

Первая проблема – это пропускная способность шины между графическим процессором и основной памятью, которая меньше, чем между основным процессором и основной памятью. Например, чипсет Intel 975X обеспечивает теоретическую пропускную способность для CPU 10.7 ГБ/с, а для GPU только 8 ГБ/с. Практика показывает, что отсутствие поддержки асинхронного ввода/вывода требует больших временных затрат для дополнительных операций, таких как блокировка/разблокировка буфера. Поскольку общие вычисления на GPU базируются на 3D рендеринге, скорость записи обычно выше, чем скорость чтения. Такая асимметрия делает процедуру считывания результата достаточно продолжительной [3, 4].

Во-вторых, общие вычисления на GPU базируются на 3D моделях, различные задачи требуют различных настроек GPU, таких как 3D модели, трансформирующие матрицы и программы шейдеров. Во время загрузки настроек вычислительные потоки GPU не задействованы. Хуже всего то, что GPU не сообщает CPU о завершении выполнения задания, поэтому CPU вынужден периодически проверять статус GPU. Это довольно времязатратная операция, так как она нарушает параллелизм между GPU и CPU.

В-третьих, недостатком GPU является производительность в логических операциях. Как известно, CPU отслеживает ветвления, GPU же работает по-другому: каждая ветка ветвления сначала выполняется, а потом уже выбирается нужный результат. Это делает распараллеливание легче, но требует больше ресурсов.

И наконец, набор инструкций GPU несовместим с CPU. Кроме того, время выполнения и длина кода лимитированы. Все это делает сложным перенос существующих алгоритмов на графические процессоры [5].

Структура разрабатываемого алгоритма

Базовый алгоритм аудио микширования состоит из пяти этапов. Первый шаг – это суммирования аудио семплов от различных источников, что может быть представлено следующей формулой [6,7]:

$$\overrightarrow{M}_t = \sum_{k=0}^{n} \vec{u}_{k,t}, \quad (1)$$

где $\vec{u}_{k,t}$ – вектор семпла, т.е. вектор отсчетов, полученных микрофоном k за время t;

$\overrightarrow{M}_t$ – итоговый вектор микширования.

Второй этап – это эхокомпенсация, которая в базовом виде заключается в исключении семпла i-го устройства из итогового вектора [8]. Данный этап представляется в виде

$$\overrightarrow{M}_{i,t} = \overrightarrow{M}_t - \vec{u}_{i,t}, \quad (2)$$

где $\overrightarrow{M}_{i,t}$ – итоговый вектор микширования для *i*-го устройства;

$\vec{u}_{i,t}$ – семпл *i*-го устройства.

Для корректности итогового вектора $\overrightarrow{M}_{i,t}$ необходимо, чтобы его размерность была равна размерности входящих векторов. Однако, после проведения этапов 1 и 2 вектор $\overrightarrow{M}_{i,t}$ может быть переполнен, что приведет к нежелательным шумам [9]. Для того, чтобы использовать изначально вектор $\overrightarrow{M}_{i,t}$ больших размеров, необходимо проводить его сжатие для дальнейшего использования. Это делается на третьем этапе по формуле

$$\overrightarrow{M}_{i,t} = \overrightarrow{M}_{i,t} \cdot l_{i,t}, \quad (3)$$

где $l_{i,t}$ – коэффициент ослабления для *i*-го устройства. Этот коэффициент необходимо вычислять автоматически, исходя из максимального сжатого семпла. Поиск максимума среди сжатых семплов происходит на четвертом этапе, а корректировка коэффициента ослабления – на пятом.

Блок-схема базового алгоритма микширования представлена на рис. 1.

Для лучшего описания алгоритма, возможности GPU представляются в виде f – функции текстуры X и координат пикселя p_i, представленной формулой

$$f(X,P) = \{y_i \mid \forall p_i \in P_i y_i = f(X, p_i)\}, \quad (4)$$

где y_i – проекция пикселя p_i на текстуру X;

P – проекция 3D-модели.

Для каждого пикселя в проекции 3D модели P будет рассчитана функция (4) и затем результат будет записан в буфер рендера.

Из формулы (4) видно, что образец вычислений на GPU может быть представлен как $A=(X, P, f)$.

Пусть n обозначает общее количество источников звука в сессии, а L – длину одного аудио семпла. Каждый из трех первых шагов микширования (накопление семплов, эхокомпенсация и сжатие) выдает n последовательностей по L байт. В то же время два последних шага (поиск максимального семпла и адаптация коэффициента затухания) выдают только n целых чисел. Поскольку первые три шага могут быть выполнены в рамках одной проекции для вычислений на GPU, они могут быть скомбинированы в один шаг, как показано ниже

$$\vec{m}_i = \left(\sum_{j=0}^{n-1} \vec{u}_j - \vec{u}_i \right) \cdot l_i. \quad (5)$$

Поскольку четвертый шаг использует другое измерение, отличное от первых трех, он не может быть объединен в рамках формулы (5). Блок-схема расширенного алгоритма микширования представлена на рис. 2.

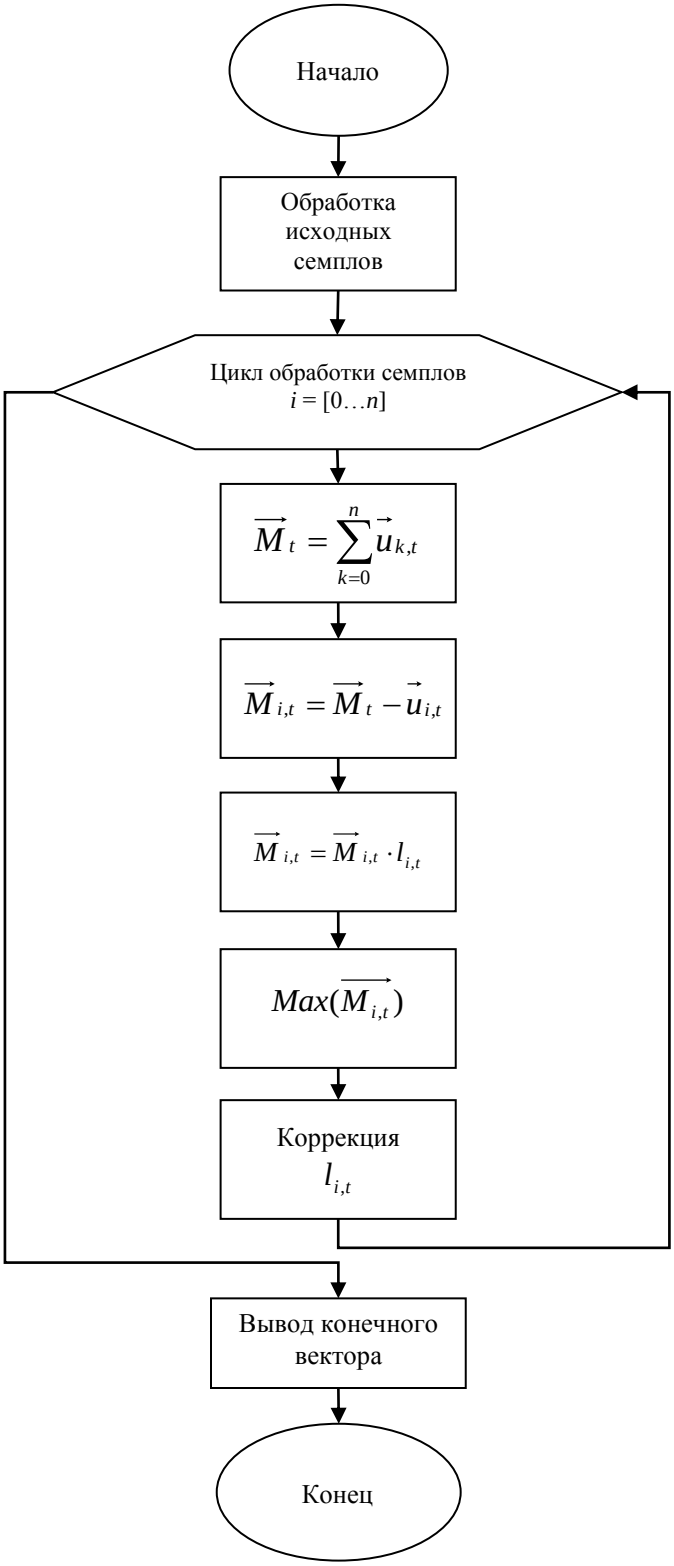


Рис. 1. Блок-схема базового алгоритма микширования

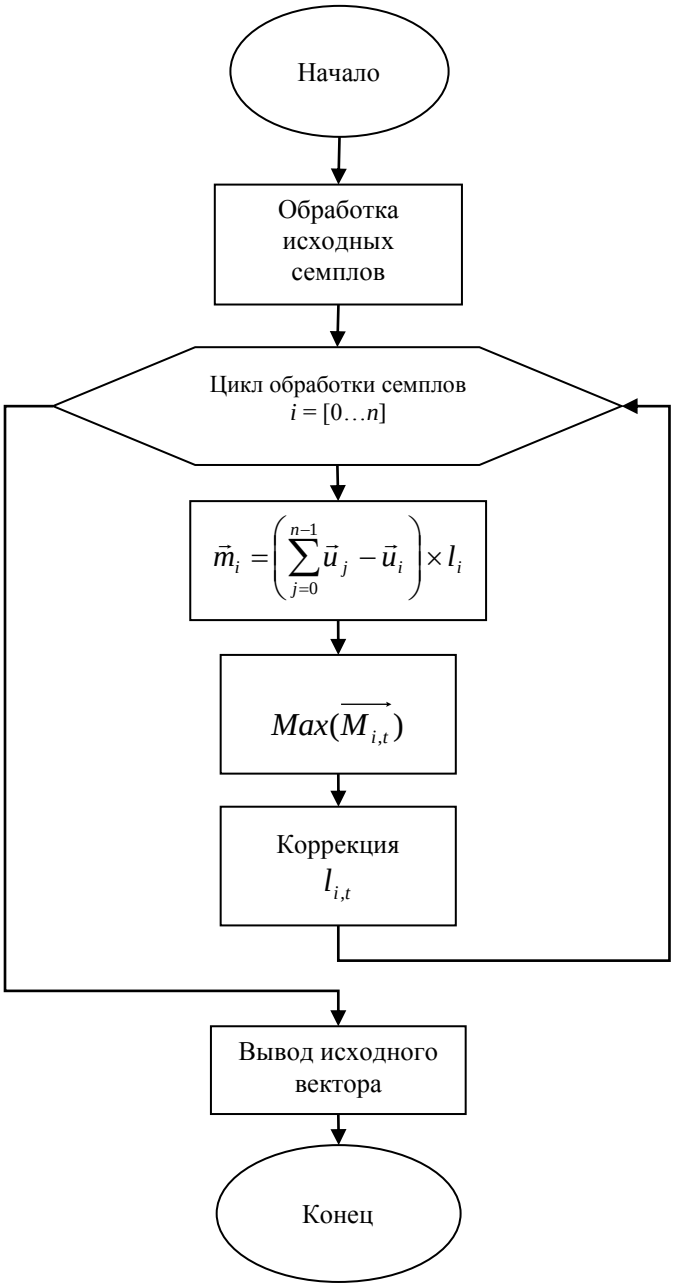


Рис. 2. Блок-схема расширенного алгоритма микширования

Обычно вычисления, проекции которых не совпадают и не имеют пересечений, могут быть объединены по общим признакам. Поэтому если эти вычисления обозначить как $A_1=(X_1, P_1, f_1)$ и $A2=(X_2, P_2, f_2)$, то их можно объединить, как показано ниже.

$$X = \langle X_1, X_2 \rangle, P = P_1 \cup P_2, \; f(\langle X_1, X_2 \rangle, p) = \begin{cases} f_1(X_1, p), p \in P_1, \\ f_2(X_2, p), p \in P_2. \end{cases} \quad (6)$$

Как видно из (6) основным алгоритмом является проверка координаты каждого пикселя для выбора функции выполнения модуля. Так как GPU выполняет все ветви до выбора нужной, каждая ветвь будет выполнена для каждого пиксела, что займет много времени.

В разрабатываемом алгоритме представлен альтернативный метод выполнения большого количества функций, который выводит в один буфер

рендера выходные данные различной длины с помощью многопотокового рендеринга. Здесь основным правилом является перемещение проекции путем модифицирования проекционной матрицы, чтобы вычислительная площадь каждой функции ограничивалась необходимой областью, а не всем буфером.

В зависимости от пикселя на него может приходиться разный объем информации без потери универсальности. Обозначим через w общее число пикселей, необходимое для хранения L байт. Таким образом, буфер рендера может быть представлен как $(w+1)n$. 3D модель разрабатываемого алгоритма представляет собой прямоугольник, который лежит на плоскости Z. Он имеет размеры: $2w/(w+1)$ единиц по ширине и 2 единицы по высоте. Координаты вершин – (-1,-1,0), (1-2/(w+1),-1,0), (-1,1,0), (1-2/(w+1),1,0).

При первом проходе рендеринга в качестве матрицы проецирования выбирается единичная матрица. Это обеспечивает проекции совпадение с 3D моделью. После преобразования видимой области, в этом проходе для выполнения первых трех шагов микширования применяется формула (5). Преобразования 3D-модели, производимые в первых трех шагах, представлены на рис. 3.

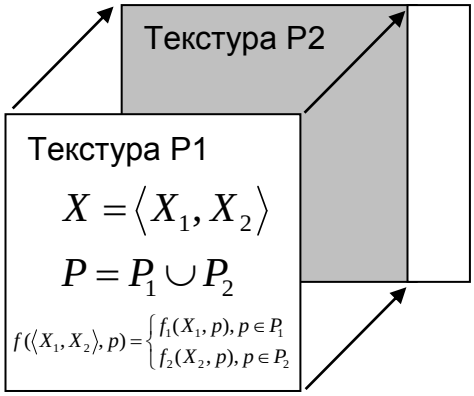


Рис. 3. Первый проход алгоритма

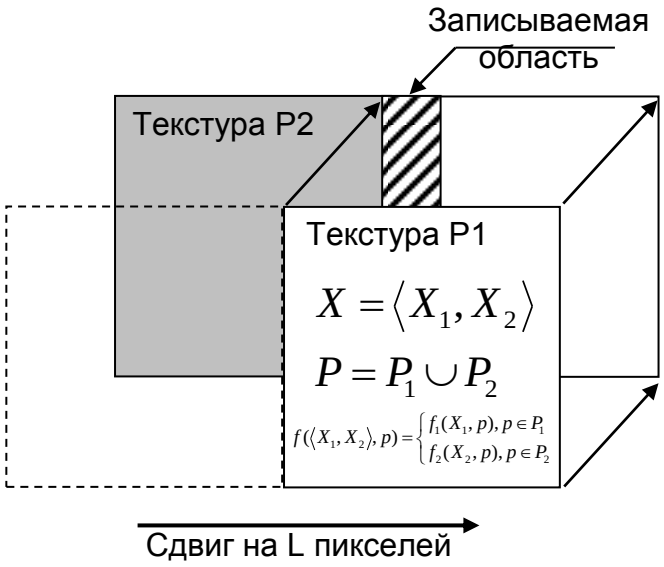


Рис. 4. Второй проход алгоритма

Во втором проходе рендеринга проекция смещается влево на L пикселей. В то же время программа шейдера переключается в режим поиска максимального семпла. В этом проходе может быть записана только одна колонка, поскольку большинство частей проекции лежат вне буфера рендера и будут автоматически игнорированы GPU. Так как отсечение проекции было выполнено в начале рендера, этот метод вызывает функцию только для корректных пикселей, а не для всего буфера. Действия, производимые на втором проходе алгоритма, представлены на рис. 4.

Использование алгоритма с одной текстурой

Как замечено выше, оба прохода алгоритма в качестве входных данных требуют n последовательностей семплов каждый. Для каждой последовательности должна быть выделена своя уникальная текстура. Всего требуется n текстур размерностью L. Такая многотекстурная технология не подходит для аудио микширования. Во-первых, для каждого источника звука требуется своя текстура. Поэтому могут потребоваться дополнительные проходы. Во-вторых, загрузка множества маленьких текстур гораздо медленнее, чем загрузка одной большой.

В разрабатываемом алгоритме предлагается загрузка единой текстуры. В качестве примера представлен первый проход алгоритма. Входные данные содержат n семплов последовательностей размером L байт и n коэффициентов затухания. Используется два текстурных буфера формата RGBA. Текстура $T1$ имеет размерность $[L/4]n$ и хранит все семплы последовательностей в линию. Текстура $T2$ имеет размерность $1 \times n$ и хранит коэффициенты затухания. Координаты всех текстур приведены в таблице 1.

Таблица 1 – Координаты текстур, используемых в разработанном алгоритме

Вершины	Координаты текстуры $T1$	Координаты текстуры $T2$
(-1, -1, 0)	(1/2w, 1)	(0.5, 1)
(1-2/(w+1), -1, 0)	(1, 1)	(0.5, 1)
(-1, 1, 0)	(1/2w, 0)	(0.5, 0)
(1-2/(w+1), 1, 0)	(1, 0)	(0.5, 0)

Аудио микширование производится независимо для каждого пикселя. Текстурные координаты пикселя (x, y) рассчитываются путем интерполяции текстурных координат вершин. Исходя из таблицы 1, текстурная координата для $T1$ должна быть (X, Y), а для $T2$ – $(0.5,Y)$. $T1$ указывает на семпл, для которого производятся текущие преобразования микширования, данный семпл назовем «точкой прицеливания». Для исключения появления эха другая текстурная координата *ptCur* ограничена по доступу $T1$. Составляющая x текстуры *ptCur* идентична текстуре $T1$, а составляющая y рассчитывается из циклической переменной, которая обозначает каждый источник звука. В цикле регистр положения v используется, чтобы пропустить «точку прицеливания». Наконец, коэффициенты затухания считываются из текстуры $T2$. Поскольку

коэффициент хранится в первом байте, выборка производится только по синей составляющей.

Экспериментальное исследование разработанного алгоритма

Тестовые входные данные для микширования представляют собой последовательности по 320 семплов. Все семплы сгенерированы случайно. В качестве тестового стенда использован компьютер с процессором Intel Core i3-4130, 4 ГБ оперативной памяти, графическая карта NVIDIA GeForce GT730. Варьировалось количество последовательностей *M*. Результаты для базового и разработанного алгоритмов на выходе идентичны. Результаты экспериментального исследования зависимости времени выполнения микширования *t* от количество последовательностей *M* приведены на рис. 5.

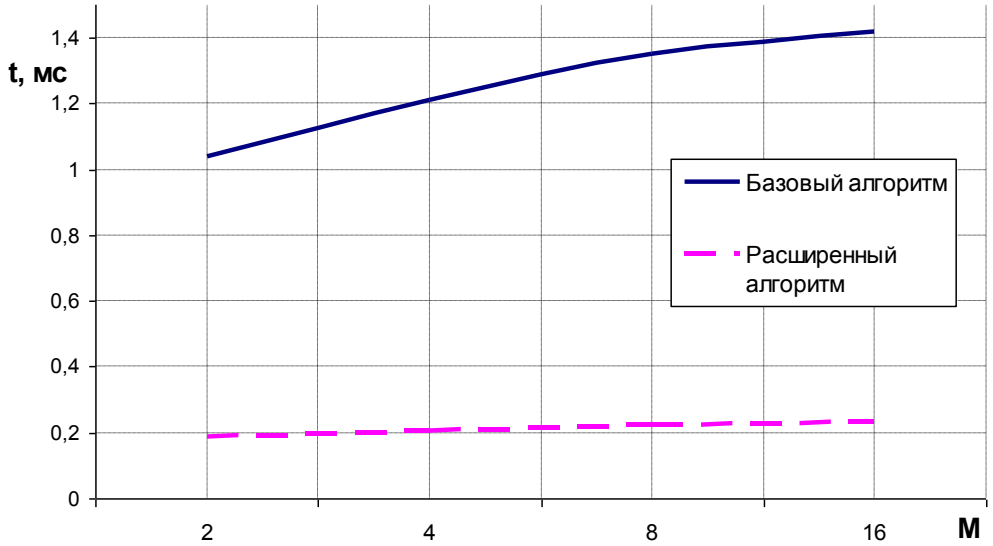


Рис. 5. Результаты экспериментального исследования зависимости времени выполнения микширования *t* от количество последовательностей *M*

Как видно из результатов тестирования, представленных на рис. 5, применение расширенного алгоритма аудио микширования позволяет увеличить производительность компьютерной системы в 5-6 раз [10, 11].

В таблице 2 приведены результаты измерения среднего времени работы алгоритма *t* для 8 случайных последовательностей по 320 семплов. В ходе измерения было проведено 1000 циклов обработки, для каждого из которых генерировались новые случайные последовательности семплов. Для полученных результатов рассчитана дисперсия выходных последовательностей, значения которой также приведены в таблице 2.

Таблица 2 – Результаты исследования алгоритма расширенного микширования аудиопотоков для 8 последовательностей семплов

Применяемый алгоритм	Среднее время работы алгоритма, мс	Дисперсия выходных последовательностей
Базовый алгоритм	1,351	3,757
Разработанный алгоритм	$2{,}226 \cdot 10^{-1}$	$1{,}426 \cdot 10^{-3}$

Как видно из результатов тестирования, представленных в таблице 2, дисперсия выходных последовательностей для базового алгоритма существенно выше, чем для разработанного. Это связано с тем, что для вычислений в графическом процессоре применяются 32-битные числа, тогда как для вычислений на центральном процессоре – 64-разрядные. Применение разработанного алгоритма в гетерогенной компьютерной системе уменьшает время на обработку данных до $0{,}2226 \cdot 10^{-3}$ с вместо $1{,}351 \cdot 10^{-3}$ с – временем обработки данных базовым алгоритмом.

Заключение

В данной работе представлен алгоритм расширенного микширования аудиопотоков для вычислений на графических процессорах. Главное его достоинство – это комбинирование множества этапов микширования путем использования двухпроходного рендера, что существенно снижает время переключения между буферами. Использование для расчетов одной текстуры повышает эффективность операций ввода/вывода. Хотя операции ввода/вывода занимают приблизительно половину времени вычислений, экспериментальные исследования разработанного алгоритма показали увеличение производительности до 6 раз.

Литература

1. Lindholm E., Nickolls J., Oberman S., Montrym J. NVIDIA Tesla: A unified graphics and computing architecture // IEEE Micro. 2008. Vol. 2. No. 28. C. 39-55.

2. Luebke D., Harris M., Kruger J., Purcell T., Govindaraju N., Buck I., Woolley C., Lefohn A.. GPGPU: general purpose computation on graphics hardware // The 31st international conference on computer graphics and interactive techniques. 2004. C. 33.

3. Колпаков А. А. Аспекты оценки увеличения производительности вычислений при распараллеливании процессоров вычислительных систем // Методы и устройства передачи и обработки информации. 2011. № 1 (13). С. 124-127.

4. Колпаков А. А. Теоретическая оценка роста производительности вычислительной системы при использовании нескольких вычислительных устройств // В мире научных открытий. 2012. № 1. С. 206-209.

5. Колпаков А. А. Оптимизация генетических алгоритмов при использовании вычислений на графических процессорах на примере задачи нулевых битовых векторов // Информационные системы и технологии. 2013. № 2 (76). С. 22-28.

6. Кропотов Ю. А. Экспериментальные исследования закона распределения вероятности амплитуд сигналов систем передачи речевой информации // Проектирование и технология электронных средств. 2006. Т. 4. С. 37-42.

7. Кропотов Ю. А. Статистические параметры сигналов при проектировании оперативно-командных телекоммуникационных систем // В мире научных открытий. 2010. № 6-1. С. 39-44.

8. Кропотов Ю. А., Быков А. А. Аппроксимация закона распределения вероятности отсчетов сигналов акустических помех // Радиотехнические и телекоммуникационные системы. 2011. № 2. С. 61-63.

9. Ермолаев В. А., Кропотов Ю. А. О корреляционном оценивании параметров моделей акустических эхо-сигналов // Вопросы радиоэлектроники. 2010. Т. 1. № 1. С. 46-50.

10. Кропотов Ю. А., Проскуряков А. Ю., Белов А. А., Колпаков А. А. Модели, алгоритмы системы автоматизированного мониторинга и управления экологической безопасности промышленных производств // Системы управления, связи и безопасности. 2015. № 2. С. 184-197.

11. Кропотов Ю. А., Белов А. А., Проскуряков А. Ю., Колпаков А. А. Методы проектирования телекоммуникационных информационно–управляющих систем аудиообмена в сложной помеховой обстановке // Системы управления, связи и безопасности. 2015. № 2. С. 165-183.

References

1. Lindholm E., Nickolls J., Oberman S., Montrym J.. NVIDIA Tesla: A unified graphics and computing architecture. *IEEE Micro*, 2008, vol. 2, no. 28, pp. 39-55.

2. Luebke D., Harris M., Kruger J., Purcell T., Govindaraju N., Buck I., Woolley C., Lefohn A.. GPGPU: general purpose computation on graphics hardware. *The 31st international conference on computer graphics and interactive techniques*, 2004, pp. 33.

3. Kolpakov A. A. Kropotov Y. A. Aspects of the assessment increase performance of computations in parallel processors of the computing system. *Metody i ustroistva peredachi i obrabotki informatsii*, 2011, vol. 13, no. 1, pp 124-127 (in Russian).

4. Kolpakov A. A. Theoretical evaluation of growth performance computing systems from the use of multiple computing devices. *V mire nauchnykh otkrytii*, 2012, no. 1, pp 206-209 (in Russian).

5. Kolpakov A. A. Optimizing the use of genetic algorithms for computing graphics processors for the problem of zero bit vector *Informatsionnye sistemy i tekhnologii*, 2013, no. 2(76), pp. 22-28 (in Russian).

6. Kropotov Y. A. Experimental study of the law of distribution of probability of amplitudes of signals of systems of transmission of voice information *Proektirovanie i tekhnologiia elektronnykh sredstv*, 2006, vol. 4, pp. 37-42 (in Russian).

7. Kropotov Y. A. The statistical parameters of the signals in the design of command-operational telecommunications systems. *V mire nauchnykh otkrytii*, 2010, no. 6-1, pp. 39-44 (in Russian).

8. Kropotov Y. A. Bykov A. A. Approximation of the law of distribution of probability of samples of the acoustic noise signals. *Radiotekhnicheskie i telekommunikatsionnye sistemy*, 2011, no. 2, pp. 61-63 (in Russian).

9. Ermolaev V. A., Kropotov Y. A. On the correlation estimation of parameters of models of acoustic echo-signals. *Voprosy radiojelektroniki*, 2010, vol. 1, no. 1, pp. 46-50 (in Russian).

10. Kropotov Y. A., Proskuryakov A. Y., Belov A. A., Kolpakov A. A. Models, Algorithms System of Automated Monitoring and Management of Ecological Safety Industrial Plants. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 184-197. Available at: http://journals.intelgr.com/sccs/archive/2015-02/08-Kropotov.pdf (accessed 24 September 2016) (in Russian).

11. Kropotov Y. A., Belov A. A., Proskuryakov A. Y., Kolpakov A. A. Methods of Designing Telecommunication Information and Control Audio Exchange Systems in Difficult Noise Conditions. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 165-183. Available at: http://journals.intelgr.com/sccs/archive/2015-02/07-Kropotov.pdf (accessed 24 September 2016) (in Russian).

Статья поступила 7 сентября 2016 г.

Информация об авторах

Колпаков Александр Анатольевич – кандидат технических наук. Доцент кафедры «Электроники и вычислительной техники». Муромский институт (филиал) «Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: параллельные и распределенные вычислительные системы. Тел.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Кропотов Юрий Анатольевич – доктор технических наук, профессор, зав. кафедрой «Электроники и вычислительной техники». Муромский институт (филиал) «Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: телекоммуникационные информационно-управляющие системы. Тел.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Алексей Анатольевич Белов – кандидат технических наук, доцент, доцент кафедры «Электроники и вычислительной техники». Муромский институт (филиал) ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: телекоммуникационные системы мониторинга и прогнозирования, обработка информации. Тел.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Наталья Евгеньевна Холкина – доцент кафедры «Электроники и вычислительной техники». Муромский институт (филиал) ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: модели и алгоритмы анализа устной речи, обработка информации. Тел.: +7 492 347 72 72. E-mail:kaf-eivt@yandex.ru

Адрес: Россия, 602264, г. Муром, ул. Орловская, д. 23.

Advanced Mixing of Audio Streams for Multi-Processor Devices in Telecommunications

A. A. Kolpakov, Y. A. Kropotov, A. A. Belov, N. E. Kholkina

Purpose. *This paper presents an algorithm enhanced mixing of audio streams for computation on GPUs. The algorithm combines multiple stages of mixing by using two-pass rendering, which significantly reduces time switching between buffers. The purpose of the present paper is development of the efficient algorithm for mixing audio streams for processing on GPUs.* ***Methods.*** *In algorithm to uses transfers operations computing on graphics processors with the use of Shader programs.* ***Novelty.*** *Novel features of presented solutions is using in algorithm with the two-pass rendering.* ***Results.*** *The results showed that the application of the developed algorithm leads to an increase in computational performance up to 6 times.* ***Practical relevance.*** *Presented solution can be implemented as software in the telecommunications multiprocessor systems.*

Key words: *two-pass rendering, algorithm of performance improving, parallel computing, heterogeneous computing system, graphics processors, mixing the audio data.*

Information about authors

Alexsandr Anatolievich Kolpakov – Ph.D. of Engineering Sciences, Associate Professor at the Department of Electronics and Computer Science. Murom Institute (branch) of the Vladimir State University named after Alexander and Nickolay Stoletovs. Field of research: parallel and distributed computing systems. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Yurij Anatolievich Kropotov – Dr. habil. of Engineering Sciences, professor, Head of Chair «Electronics and Computer Science». Murom Institute (branch) of the Vladimir State University named after Alexander and Nickolay Stoletovs. Field of research: telecommunication information and control systems. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Alexey Anatolievich Belov – Ph.D. of Engineering Sciences, Associate Professor, Associate Professor at the Department of «Electronics and Computer Science». Murom institute (branch) of the «Vladimir State University named after Alexander and Nickolay Stoletovs». Field of research: telecommunications monitoring and forecasting system, information processing. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Natal'ia Evgen'evna Kholkina – Associate Professor at the Department of Electronics and Computer Science. Murom institute (branch) of the Vladimir State University named after Alexander and Nickolay Stoletovs. Field of research: models and algorithms of speech analysis, information processing. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Address: Russia, 602264, Murom, st. Orlovskaya, h. 23.

УДК 62–50:519.7/8

Полиинтервалы, их исчисление и применение

Левин В.И.

Актуальность. *В последние десятилетия в военной и гражданской сферах все чаще встречаются новые технологии, связанные с изучением неопределенности. Эти технологии широко применяются в технике, экономике, социальной сфере. Для их поддержки необходимы новые математические модели и методы. В связи с этим данная статья, посвященная разработке новой модели неопределенности (полиинтервал) и математических методов ее изучения, является актуальной.* ***Цель статьи*** *заключается в детальной разработке новой математической модели неопределенности – полиинтервала, являющегося последовательностью конечного числа интервалов неопределенности, системы алгебраических операций над полиинтервалами и правил выполнения этих операций.* ***Метод.*** *Для выполнения поставленной цели предложено распространить на изучение полиинтервалов известный в интервальной математике метод изучения интервалов, основанный на определении алгебраических операций над интервалами в виде теоретико-множественных обобщений соответствующих операций над вещественными числами.* ***Новизна.*** *Новизна работы заключается в предложенной новой математической модели неопределенности систем в виде полиинтервалов, совместно с математическим аппаратом, позволяющим выполнять различные операции над полиинтервалами и тем самым дающим возможность выполнять математическое моделирование систем с неопределенностью.* ***Результат****. В статье детально разработана новая математическая модель неопределенности – полиинтервал. Определена система алгебраических операций над полиинтервалами и выведены правила их выполнения. Дан алгоритм изучения неопределенных систем с полиинтервальными параметрами.*

Ключевые слова: *интервал, полиинтервал, неопределенность, алгебра полиинтервалов, моделирование систем.*

Введение

Известно, что в период Второй мировой войны в практику ведения военных действий было введено множество новых технологий: обнаружение воздушных целей с помощью радаров, управление огнем зенитной артиллерии, шифровка и дешифровка информации, атомное оружие и т.д. Все эти технологии в той или иной степени были связаны с изучением неопределенности, присущей любым военным действиям, и использовали соответствующие математические методы, в первую очередь, теорию вероятностей. После войны эти работы были продолжены и распространены на гражданскую сферу – экономику, технику, социум. При этом расширилось само понимание неопределенности, в которую теперь стали включать не только случайность возможных исходов, но и их неединственность или их незнание, дрейф переменных, семантическую неопределенность целей, многокритериальность при принятии решений, недоопределенность модели или структуры изучаемой системы и т.д. Новые подходы к описанию неопределенности изучаемых систем привели к появлению новых математических методов для их изучения: теория нечетких множеств, многозначная логика, теория сверхслучайных процессов и др. Одним из наиболее популярных методов стала интервальная математика, занимающаяся изучением

величин, определяемых с точностью до интервалов возможных значений [1, 2]. Но одиночные интервалы, являющиеся объектом изучения в интервальной математике, не охватывают всех ситуаций, встречающихся на практике. Например, неопределенный период времени, в течение которого возможно успешное проведение военной операции, может включать несколько последовательных временных интервалов, скажем $([4^{00},5^{30}],[21^{00},23^{00}],[24^{00},2^{00}])$. Аналогично, участок пространства, в рамках которого возможно наблюдение некоторых объектов, может включать в себя несколько последовательных угловых интервалов, скажем $([15^{\circ},21^{\circ}],[28^{\circ},35^{\circ}],[48^{\circ},53^{\circ}])$. Очевидным образом, на практике могут появляться и другие подобные примеры. Во всех таких примерах мы сталкиваемся с новыми неопределенными объектами, которые имеют вид последовательностей интервалов неопределенности. Каждый такой объект естественно назвать полиинтервалом. Настоящая статья полностью посвящена теории и возможным применениям полиинтервалов.

1. Постановка задачи

Распространенный подход к изучению неопределенных систем, известный под названием интервальной математики [1, 2], строится на базе понятия интервала, трактуемого как множество всех возможных значений неполностью определенной величины $\tilde{a}$, задаваемой лишь ее нижней a_1 и верхней a_2 границами. Величину $\tilde{a}$ можно записать в виде следующего ограниченного интервала неопределенности

$$\tilde{a} \equiv [a_1, a_2] = \{a \mid a_1 \le a \le a_2\}. \qquad (1)$$

Здесь предполагается, что неизвестное «истинное» значение неопределенной величины $\tilde{a}$ достоверно лежит в пределах интервала $[a_1, a_2]$, не выходя за его границы a_1 и a_2. Причем все значения в пределах этого интервала считаются «равновозможными» в том смысле, что нет никаких оснований предпочитать одно значение другому. Заметим, что в данном случае понятие равновозможности не означает задание равномерного вероятностного или какого-либо иного распределения возможных значений внутри указанного интервала. Над интервалами вида (1) вводятся алгебраические операции, аналогичные соответствующим операциям над числами. Для этого используется теоретико-множественная конструкция

$$\tilde{a} \circ \tilde{b} = \{a \bullet b \mid a \in \tilde{a}, b \in \tilde{b}\}, \quad \circ \tilde{a} = \{\bullet a \mid a \in \tilde{a}\}. \qquad (2)$$

т.е. любая операция над интервалами $\circ$ определяется на основе соответствующей операции над точными величинами $\bullet$, при условии, что конкретные значения этих величин пробегают все возможные значения из

соответствующих интервалов. Из этого определения вытекают простые правила выполнения операций над интервалами:

$$
\begin{aligned}
&[a_1,a_2]+[b_1,b_2]=[a_1+b_1,a_2+b_2];\\
&[a_1,a_2]-[b_1,b_2]=[a_1-b_2,a_2-b_1];\\
&k\cdot[a_1,a_2]=\begin{cases}[ka_1,ka_2], & k>0,\\ [ka_2,ka_1], & k<0;\end{cases}\\
&[a_1,a_2]\cdot[b_1,b_2]=[\min_{i,j}(a_i\cdot b_j),\max_{i,j}(a_i\cdot b_j)];\\
&[a_1,a_2]/[b_1,b_2]=[a_1,a_2]\cdot[1/b_2,1/b_1],\ \text{при}\ 0\notin[b_1,b_2].
\end{aligned}
\tag{3}
$$

Мы продолжим развитие интервальной математики, введя понятие полиинтервала как последовательности нескольких одиночных интервалов неопределенности

$$\tilde{A}=(\tilde{a},\tilde{b},...,\tilde{d}), \tag{4}$$

где $\tilde{a},\tilde{b},...,\tilde{d}$ – одиночные интервалы вида (1).

Операции над полиинтервалами введем аналогично операциям над интервалами, т.е. с помощью теоретико-множественной конструкции типа (2)

$$\tilde{A}\circ\tilde{B}=\{a\bullet b\,|\,a\in\tilde{A},b\in\tilde{B}\},\quad \circ\tilde{A}=\{\bullet a\,|\,a\in\tilde{A}\}. \tag{5}$$

Здесь $\tilde{A}$ – полиинтервал вида (4), $\tilde{B}$ – другой полиинтервал того же вида, но с другими составляющими его одиночными интервалами вида (1). Задача работы заключается в том, чтобы на базе определения (5) операций над полиинтервалами вывести правила выполнения указанных выше операций, аналогичные правилам (3) выполнения операций над интервалами.

2. Математический аппарат

Будем представлять полиинтервалы (4) в теоретико-множественных терминах таким образом:

$$\tilde{A}=\tilde{a}\cup\tilde{b}\cup...\cup\tilde{d}. \tag{6}$$

Пусть заданы два полиинтервала $\tilde{A}$ и $\tilde{B}$ следующего вида

$$\tilde{A}=\bigcup_{i=1}^{m}\tilde{a}^i,\quad \tilde{B}=\bigcup_{j=1}^{n}\tilde{b}^j, \tag{7}$$

где $\tilde{a}^i=[a_1^i,a_2^i],\ i=\overline{1,m}$ и $\tilde{b}^j=[b_1^j,b_2^j],\ j=\overline{1,n}$ – одиночные интервалы, составляющие $\tilde{A}$ и $\tilde{B}$ соответственно. Требуется выполнить операцию $\circ$ над этими полиинтервалами. Согласно определению (5) имеем с учетом вида (7) полиинтервалов $\tilde{A}$ и $\tilde{B}$

$$\tilde{A}\circ\tilde{B}=\{a\bullet b\,|\,a\in\bigcup_{i=1}^{m}\tilde{a}^i,b\in\bigcup_{j=1}^{n}\tilde{b}^j\}. \tag{8}$$

На основании ассоциативного закона алгебры множеств выражение (8) можно представить как

$$\tilde{A}\circ\tilde{B}=\bigcup_{i=1}^{m}\bigcup_{j=1}^{n}\{a\bullet b\,|\,a\in\tilde{a}^i,b\in\tilde{b}^j\}. \tag{9}$$

Однако, согласно определению (2) выражение в фигурных скобках формулы (9) равно $\tilde{a}^i \circ \tilde{b}^j$. Так что окончательно получаем

$$\tilde{A} \circ \tilde{B} = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} (\tilde{a}^i \circ \tilde{b}^j),$$

или в развернутом виде

$$\left(\bigcup_{i=1}^{m} \tilde{a}^i \right) \circ \left(\bigcup_{j=1}^{n} \tilde{b}^j \right) = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} (\tilde{a}^i \circ \tilde{b}^j) \qquad (10)$$

Выражение для операции $\circ$ над одним полиинтервалом $\tilde{A}$ вида (7) имеет вид, аналогичный (10)

$$\circ \tilde{A} = \bigcup_{i=1}^{m} (\circ \tilde{a}^i)$$

или в развернутом виде

$$\circ \left(\bigcup_{i=1}^{m} \tilde{a}^i \right) = \bigcup_{i=1}^{m} (\circ \tilde{a}^i). \qquad (11)$$

Формулы (10), (11) сводят выполнение операций над полиинтервалами к выполнению тех же самых операций над одиночными интервалами. Поскольку для последних имеются формулы их конструктивного выполнения (3), то путем совместного применения формул (3), (10), (11) решается и поставленная задача конструктивного выполнения различных операций над полиинтервалами.

3. Решение задачи

Установим сначала вид формулы для конструктивного выполнения операции сложения полиинтервалов. Для этого подставим в исходную формулу (10) выражения сумм интервалов согласно (3) и учтем, что в этом случае операция $\circ$ есть сложение +. В результате получим искомую формулу в следующем виде

$$\tilde{A} + \tilde{B} = \bigcup_{i=1}^{m} [a_1^i, a_2^i] + \bigcup_{j=1}^{n} [b_1^j, b_2^j] = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} [a_1^i + b_1^j, a_2^i + b_2^j]. \qquad (12)$$

Аналогично устанавливается формула для конструктивного выполнения операции вычитания полиинтервалов. Для этого подставляем в исходную формулу (10) выражения разностей интервалов согласно (3), при этом учитывая, что здесь операция $\circ$ есть вычитание –. В результате мы получаем формулу

$$\tilde{A} - \tilde{B} = \bigcup_{i=1}^{m} [a_1^i, a_2^i] - \bigcup_{j=1}^{n} [b_1^j, b_2^j] = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} [a_1^i - b_2^j, a_2^i - b_1^j]. \qquad (13)$$

Формула для конструктивного выполнения операции умножения полиинтервала на число находится аналогично. При этом используем выражение произведения интервала на число (3), а в качестве исходной формулы используем не (10), а (11).

В результате находим

$$k\tilde{A} = k\left(\bigcup_{i=1}^{m}[a_1^i, a_2^i]\right) = \begin{cases} \bigcup_{i=1}^{m}[ka_1^i, ka_2^i], & k > 0, \\ \bigcup_{i=1}^{m}[ka_2^i, ka_1^i], & k < 0. \end{cases} \quad (14)$$

Аналогично формулам (12), (13) для конструктивного выполнения операций сложения и вычитания полиинтервалов находим формулы для конструктивного выполнения операций умножения и деления полиинтервалов. При этом опираемся на правила умножения и деления интервалов (3), но в качестве исходной формулы снова используем формулу (10). В результате получаем формулу умножения полиинтервалов в виде

$$\bigcup_{i=1}^{m}[a_1^i, a_2^i]\cdot\bigcup_{j=1}^{n}[b_1^j, b_2^j] = \bigcup_{i=1}^{m}\bigcup_{j=1}^{n}[a_1^i, a_2^i]\cdot[b_1^j, b_2^j] = \bigcup_{i=1}^{m}\bigcup_{j=1}^{n}\left[\min_{s,q}(a_s^i b_q^j), \max_{s,q}(a_s^i b_q^j)\right] \quad (15)$$

и формулу деления полиинтервалов в виде

$$\bigcup_{i=1}^{m}[a_1^i, a_2^i] \Big/ \bigcup_{j=1}^{n}[b_1^j, b_2^j] = \bigcup_{i=1}^{m}\bigcup_{j=1}^{n}[a_1^i, a_2^i]\cdot[1/b_2^j, 1/b_1^j] = \bigcup_{i=1}^{m}\bigcup_{j=1}^{n}\left[\min_{s,q}(a_s^i / b_q^j), \max_{s,q}(a_s^i / b_q^j)\right] \quad (16)$$

при $0 \notin [b_1^j, b_2^j], \quad j = \overline{1,n}.$

Формулы (12)–(16) дают правила конструктивного выполнения всех введенных выше алгебраических операций над полиинтервалами путем сведения указанных операций к соответствующим хорошо известным операциям над одиночными интервалами.

Теперь алгоритм решения разнообразных задач, возникающих при исследовании систем с полиинтервальными характеристиками, можно представить следующим образом.

Шаг 1. Построение математической модели, представляющей решение задачи как вычисление и анализ функции F аргументов-полиинтервалов.

Шаг 2. Составление по построенной модели блок-схемы алгоритма вычисления (анализа) функции F.

Шаг 3. Вычисление (анализ), по имеющейся блок-схеме алгоритма, полиинтервальной функции F, с использованием формул (12)–(16) выполнения различных операций над полиинтервалами. Заметим, что заключительной операцией во всех формулах является объединение интервалов, выполняемое известными методами [3].

Пример. Работник служит в двух фирмах: A и B. Причем в фирме A его месячная заработная плата в зависимости от заказов оценивается в размере 10000 ± 1000 руб. или 15000 ± 1500 руб. В фирме B его месячная зарплата оценивается (также в зависимости от заказов) в размере 3000 ± 500 руб. или же 8000 ± 1000 руб. Оценить суммарную месячную зарплату работника.

Решение. *Шаг 1.* В фирме A 1-ю зарплату можно представить в виде интервала $[a_1^1, a_2^1] = [9000, 11000]$, 2-ю – как интервал $[a_1^2, a_2^2] = [13500, 16500]$. Аналогично этому, в фирме B 1-ю зарплату можно представить в виде интервала $[b_1^1, b_2^1] = [2500, 3500]$, а 2-ю – в виде интервала $[b_1^2, b_2^2] = [7000, 9000]$. Итак,

месячную зарплату в фирмах A и B можно представить соответственно следующими полиинтервалами

$$\tilde{A} = \bigcup_{i=1}^{2} [a_1^i, a_2^i] = [9000,11000] \cup [13500,16500],$$

$$\tilde{B} = \bigcup_{j=1}^{2} [b_1^j, b_2^j] = [2500,3500] \cup [7000,9000].$$

Месячная суммарная зарплата работника $\tilde{C}$ равна сумме его месячных зарплат в фирмах A и B, т.е. $\tilde{C} = \tilde{A} + \tilde{B}$. После подстановки значений полиинтервалов $\tilde{A}$ и $\tilde{B}$ получаем

$$\tilde{C} = \bigcup_{i=1}^{2} [a_1^i, a_2^i] + \bigcup_{j=1}^{2} [b_1^j, b_2^j] =$$

$$= ([9000,11000] \cup [13500,16500]) + ([2500,3500] \cup [7000,9000]).$$

Последняя формула и есть математическая модель решения задачи в виде вычисления суммы двух полиинтервалов.

Шаг 2. Блок-схема алгоритма вычисления функции-модели, полученной на шаге 1 алгоритма, очевидна и содержит всего одну ступень, на которой вычисляется сумма двух полиинтервалов.

Шаг 3. Вычисляем полиинтервальную функцию-модель, полученную на шаге 1. Эта функция – сумма двух полиинтервалов, содержащих каждый два интервала. По формуле (12) сложения полиинтервалов находим

$$\tilde{C} = \bigcup_{i=1}^{2} [a_1^i, a_2^i] + \bigcup_{j=1}^{2} [b_1^j, b_2^j] =$$

$$= [a_1^1 + b_1^1, a_2^1 + b_2^1] \cup [a_1^1 + b_1^2, a_2^1 + b_2^2] + [a_1^2 + b_1^1, a_2^2 + b_2^1] \cup [a_1^2 + b_1^2, a_2^2 + b_2^2],$$

что после подстановки численных значений переменных a_k^i, b_s^j дает

$$\tilde{C} = [9000 + 2500,11000 + 3500] \cup [9000 + 7000,11000 + 9000] \cup$$

$$\cup [13500 + 2500,16500 + 3500] \cup [13500 + 7000,16500 + 9000] =$$

$$= [11500,14500] \cup [16000,20000] \cup [16000,20000] \cup [20500,25500] =$$

$$= [11500,14500] \cup [16000,20000] \cup [20500,25500].$$

Таким образом, суммарная месячная зарплата работника, в зависимости от заказов у фирм $\tilde{A}$ и $\tilde{B}$, может лежать в интервалах $[11500,14500]$ или $[16000,20000]$ или $[20500,25500]$ рублей или, в другой форме записи, составлять 13000 ± 1500 или 18000 ± 2000 или 23000 ± 2500 рублей.

4. Обсуждение

Как показано выше, дальнейшее развитие концепции интервальной неопределенности приводит к понятию полиинтервала, характеризующего более сложную неопределенность, имеющую вид последовательности интервалов неопределенности. Такая неопределенность характеризуется тем, что параметр системы не просто принимает какое-то, заранее неизвестное, значение внутри определенного заданного интервала, но еще сначала выбирает какой-нибудь,

заранее неизвестный, интервал из нескольких заданных интервалов, внутри которого затем принимает какое-то, заранее неизвестное значение. Эта более сложная модель неопределенности встречается очень часто в военном деле, экономике, технике и иных областях и потому заслуживает изучения и разработки. Логично осуществлять эту разработку, используя подходы интервальной математики [1, 2] и развивая их в направлении учета многоинтервальности. Подобно тому, как интервальная математика базируется на алгебре интервалов, полиинтервальная математика базируется на алгебре полиинтервалов. Однако, в отличие от алгебры интервалов, в алгебре полиинтервалов не имеется простых зависимостей между сложностью (длиной) операндов и сложностью результата операции. Это вызвано большей сложностью неопределенных систем, описываемых алгеброй полиинтервалов.

Заключение

В статье сформулирована задача изучения новой модели неопределенности – так называемого полиинтервала, обобщающей известную модель неопределенности – интервал – на случай существования нескольких последовательных интервалов неопределенности. С помощью известной из интервальной математики теоретико-множественной конструкции, аналогично операциям над интервалами, введены операции над полиинтервалами. Разработана методика сведения операций над интервалами к операциям над полиинтервалами. С ее помощью выведены формулы для конструктивного выполнения всех операций над полиинтервалами и построен соответствующий алгоритм. На примере из области экономики проиллюстрирована практическая польза разработанной теории и методов.

Литература

1. Алефельд Г., Херцбергер Ю. Введение в интервальные вычисления. – М: Мир, 1987. – 370 с.

2. Левин В. И. Интервальная математика и исследование систем в условиях неопределенности. – Пенза: Изд-во Пензенского технологического института, 1998. – 55 с.

3. Столл Р. Р. Множества. Логика. Аксиоматические теории. – М.: Просвещение, 1968. – 232 с.

References

1. Alefeld, G., Herzberger, Ju., *Einführung in die Intervallrechnung* [Introduction to the Interval Computations]. Zürich, B.I.-Wissenschaftsverlag, 1974. 398 p. (in German).

2. Levin V. I. *Intervalnaya matematika i issledovanie system v usloviyah neopredelennosti* [Interval Mathematics and Research of Systems in Condition of Uncertainty]. Penza, Penza Technological Institute Publishing, 1998. 55 p. (in Russian).

3. Stoll R. R. *Sets, Logic and Axiomatic Theories*. San Francisco, W.H. Freeman and Co., 1961, 206 p.

Информация об авторе

Левин Виталий Ильич – доктор технических наук, профессор, PhD, Full Professor. Заслуженный деятель науки РФ. Пензенский государственный технологический университет. Область научных интересов: логика; математическое моделирование в технике, экономике, социологии, истории; принятие решений; оптимизация; теория автоматов; теория надежности; распознавание; история науки; проблемы образования. E-mail: vilevin@mail.ru

Адрес: 440039, Россия, г. Пенза, пр. Байдукова/ул. Гагарина, д. 1а/11.

Polyintervals: Calculus and Applications

V. I. Levin

Relevance. *In recent decades there are more and more new technologies in the military and civilian spheres which associated with studying of uncertainty. These technologies are widely used in engineering, economics, social sphere. To support their new mathematical models and methods are needed. In this regard, this article dedicated to the development of new model of uncertainty (polyinterval) and mathematical methods of its study is relevant.* ***The purpose*** *of the article is in the detailed design of a new adequate mathematical model of uncertainty - polyinterval, which is a sequence of a finite number of intervals of uncertainty, the system of algebraic operations on polyintervals and rules to perform these operations.* ***Method.*** *To accomplish this goal we propose to extend to study polyintervals the method from the interval mathematics based on the determination of algebraic operations on intervals in form of set-theoretic generalizations of operations on real numbers.* ***Novelty.*** *The novelty of the work lies in the proposed new mathematical model of uncertainty in form of systems of polyintervals, together with mathematical tools allowing to perform various operations on polyintervals and thereby enabling them to perform mathematical modeling of uncertain systems.* ***Result.*** *The article detailed developed a new mathematical model of uncertainty – polyinterval. The system of algebraic operations on polyintervals is determined and rules for their implementation are output. The algorithm of study of uncertain systems with polyinterval parameters is given.*

Keywords *interval value, polyinterval value, uncertainty, algebra of polyinterval values, system modeling.*

Information about Author

Vitaly Ilyich Levin – the Doctor of Engineering Sciences, Professor, PhD, Full Professor. Honored worker of science of the Russian Federation. Penza State Technological University. Field of Research: logic; mathematical modeling in technics, economy, sociology, history; decision-making; optimization; automata theory; theory of reliability; history of science; problems of education. E-mail: vilevin@mail.ru

Address: 440039, Russia, Penza, pr. Baydukova / Gagarin st., 1a/11.

УДК 004.021

Повышение производительности многопроцессорных вычислительных систем с гетерогенной архитектурой

Колпаков А. А., Кропотов Ю. А., Проскуряков А. Ю.

Постановка задачи. *Вопрос создания высокопроизводительных вычислительных комплексов на базе компьютерных систем является актуальным, так как объемы обрабатываемой информации, вычислений и исследований с большими массивами данных постоянно увеличиваются. В связи с этим возникает задача разработки алгоритмов повышения производительности компьютерных систем на основе архитектуры использующих дополнительные вычислительные производительные модули или с однородные модули на графических процессорах.* ***Целью работы*** *является разработка алгоритма повышения производительности параллельных вычислений в многопроцессорных вычислительных системах с гетерогенной архитектурой.* ***Используемые методы:*** *метод декомпозиции задачи на этапы, метод принятия решений о переносе вычислений на графические процессоры.* ***Новизна.*** *Элементами новизны представленного решения является модифицированная PRAM-модель для применения графических процессоров.* ***Результат.*** *Разработан алгоритм повышения производительности параллельных вычислений в многопроцессорных вычислительных системах с гетерогенной архитектурой. Данный алгоритм использует применение графических процессоров в качестве специализированных вычислительных модулей в составе гетерогенной многопроцессорной вычислительной системы. Его применение приводит к существенному повышению производительности вычислений в зависимости от числа обрабатываемых потоков.* ***Практическая значимость****. Представленное решение предполагается реализовать в виде программного модуля для компьютерной системы с использованием технологии CUDA.*

Ключевые слова: *параллельные вычисления, алгоритм повышения производительности вычислений, PRAM-модель, гетерогенные вычислительные системы, графические процессоры.*

Введение

Известно, что повышение эффективности вычислительных компьютерных систем осуществляется в зависимости от организации процесса решения задач [1, 2]. В общем случае задачи представляются параллельными программами и описываются рядом параметров, в числе которых: количество ветвей, ранг необходимой подсистемы, время решения и т.п. Режим функционирования высокопроизводительных вычислительных систем формируется мультипрограммным методом или в некоторых вычислительных компьютерных системах используется частичное применение вычислительных модулей, что в недостаточной степени обеспечивает повышение производительности вычислений [3].

В связи с этим возникает задача разработки методов повышения производительности компьютерных систем на основе модели архитектуры с использованием дополнительных вычислительных производительных модулей или с использованием однородных модулей на графических процессорах. Основной задачей повышения производительности такой вычислительной системы является решение проблемы принятия решений о переносе операций вычислений на специализированные вычислительные модули и кэшировании данных, что требует исследований и разработки соответствующих алгоритмов [4].

Архитектура гетерогенных многопроцессорных вычислительных систем

Для рассмотрения особенностей обобщенной архитектуры специализированных вычислительных модулей и их взаимодействия с центральным процессором была разработана и исследована структурная схема архитектуры гетерогенной многопроцессорной вычислительной системы, которая изображена на рис. 1. Базовыми структурными элементами специализированных вычислительных модулей являются спецпамять (SpRAM), в которой отдельно можно выделить память констант и глобальную память, и множество мультипроцессоров. Чтобы обработать данные на специализированных вычислительных модулях, необходимо передать их из оперативной памяти компьютера в SpRAM в соответствии со структурной схемой архитектуры гетерогенной системы на рис. 1.

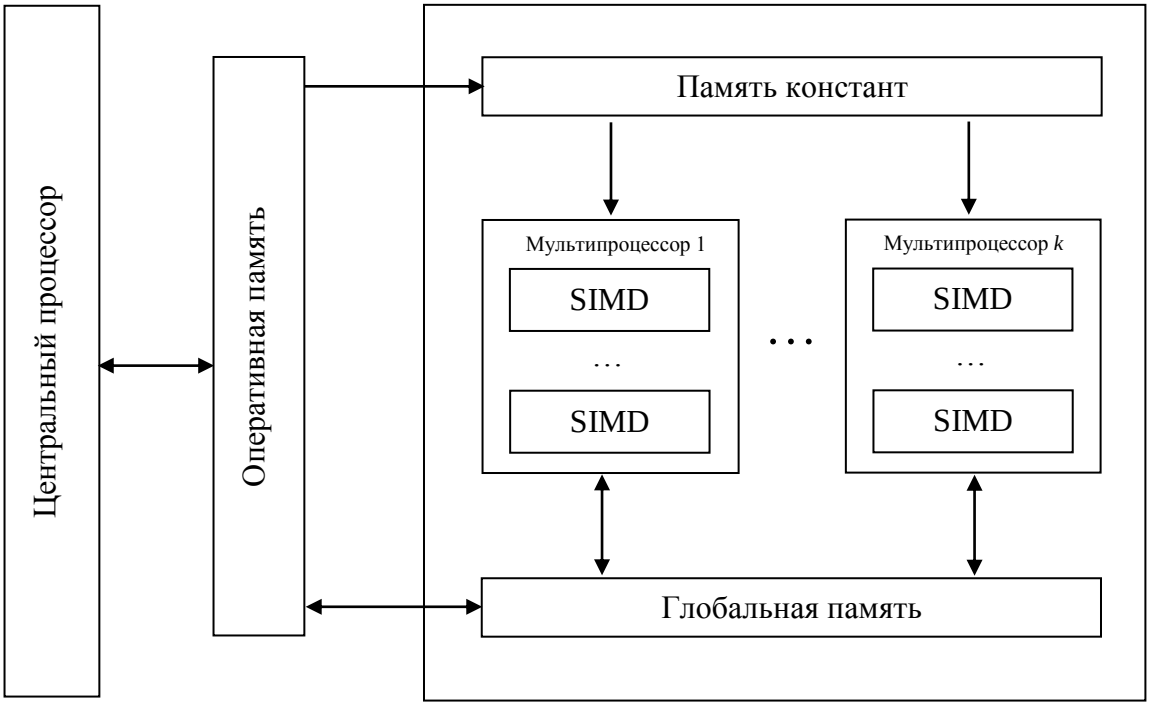


Рис. 1. Структурная схема архитектуры гетерогенной многопроцессорной вычислительной системы

Как видно из структурной схемы на рис. 1, связку «центральный процессор – графический процессор» можно отнести к модели с общей памятью. Основной моделью с общей памятью является модель PRAM (parallel random-access machine) – машина с параллельным произвольным доступом. Она является абстрактной идеализированной моделью параллельной синхронной машины с разделяемой общей памятью, которая использует допущения, приведенные ниже:

- количество процессоров (q) в машине не ограничено;
- каждый процессор имеет равнозначный доступ к любой ячейке общей памяти, размер которой не ограничен;
- отсутствует конкуренция по ресурсам;

– процессоры работают в режиме MIMD, но в частном случае может использоваться режим SIMD.

Все процессоры исполняют инструкции синхронно, причем выполнение любой инструкции занимает ровно 1 такт, называемый шагом PRAM-машины.

Чтобы оценить время выполнения алгоритма для N входных данных на PRAM-машине с p потоками, в работе [5] было получено выражение

$$T(N,p) = O\left(\frac{W(N)}{p} + S(N)\right), \quad (1)$$

где O – верхняя асимптотическая оценка трудоёмкости алгоритма,

N – количество входных данных алгоритма,

$S(N)$ – шаговая сложность алгоритма,

$W(N) = \sum_{i=1}^{S(n)} W_i(N)$ – рабочая сложность параллельного алгоритма, где $W_i(N)$ – количество параллельных операций на шаге i.

Формула (1) дает верхнюю асимптотическую оценку времени исполнения алгоритма с шаговой сложностью $S(N)$ и рабочей сложностью $W(N)$.

Из схемы, приведенной на рис. 1, можно отметить, что PRAM модель может быть применена к многопроцессорной системе с учётом следующих уточнений и дополнений:

1) все процессоры могут одновременно считывать данные из разделяемой памяти, но запись должна быть монопольной, т.к. порядок изменения ячейки разделяемой памяти при обращении на запись из нескольких скалярных процессоров не определён (PRAM – CREW (Concurrent Read, Exclusive Write));
2) количество скалярных процессоров в графическом мультипроцессоре ограничено сверху (q_{max} процессоров). Для выполнения большего числа потоков используется система горизонтального параллелизма, аналогичная горизонтальной структуре в модели BSP: генерируется расписание последовательного исполнения потоков, разбитых на пучки по q_{warp} скалярных процессоров;
3) размер разделяемой памяти мультипроцессора ограничен – M_s байт;
4) все скалярные процессоры работают с одинаковой скоростью по принципу SIMD со скоростью S_{GPU} элементарных операций в секунду;
5) должна иметь место дополнительная операция – обращение к оперативной памяти SpRAM специализированного вычислительного модуля на чтение или запись. Задержка при обращении K определяется количеством элементарных операций, требуемых при обращении к одному числу одинарной точности в глобальной памяти специализированного вычислительного модуля.

Таким образом, PRAM модель с перечисленными уточнениями и дополнениями допускает применение графических процессоров в качестве специализированных вычислительных модулей для общих вычислений.

Общий алгоритм оптимизации параллельных вычислений в многопроцессорных вычислительных системах с гетерогенной архитектурой

Для организации параллельных вычислений в многопроцессорных вычислительных системах с гетерогенной архитектурой «CPU – SCM», был разработан общий алгоритм оптимизации, который приведен на рис. 2. В качестве специализированного вычислительного модуля используется графический процессор GPU.

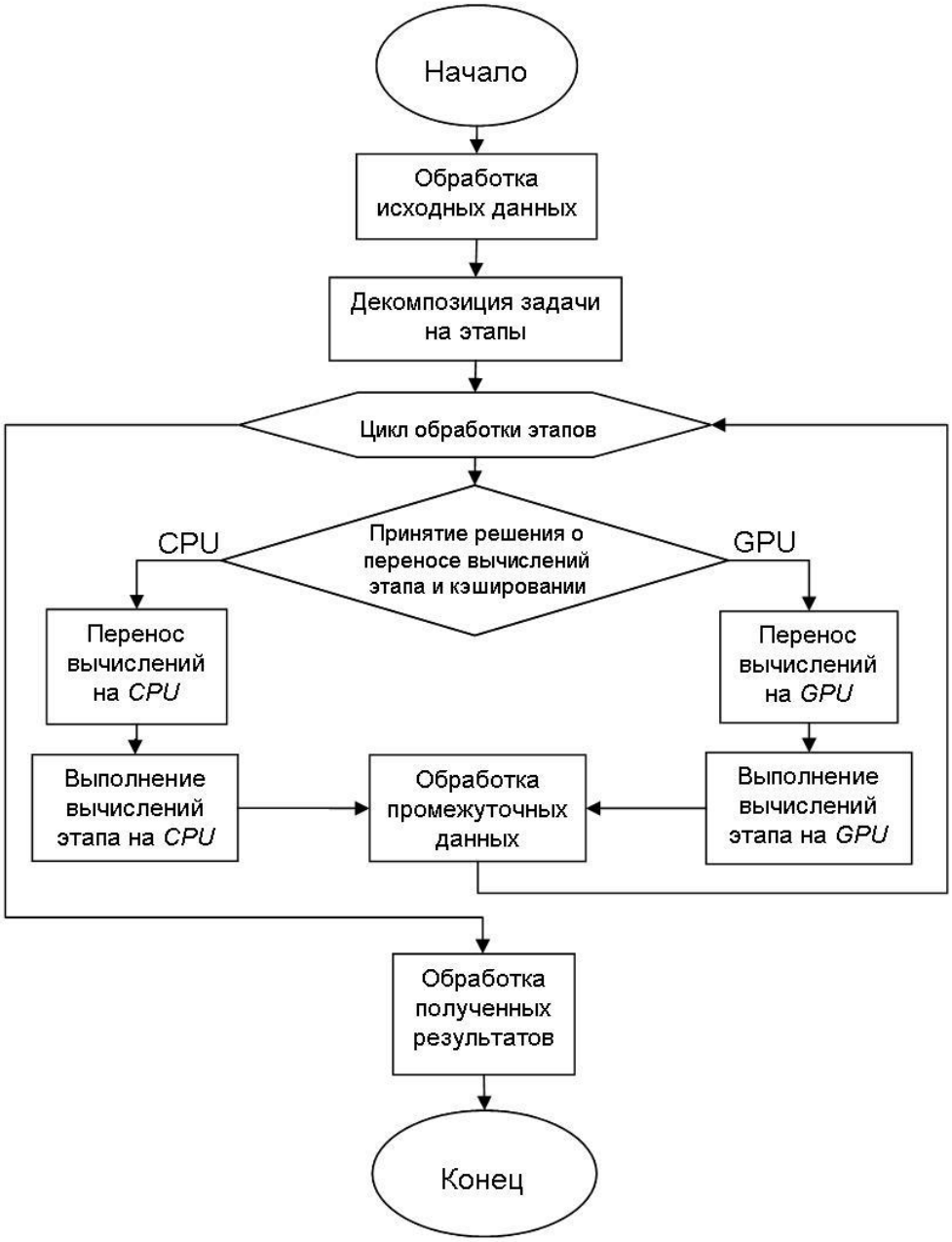


Рис. 2. Алгоритм повышения производительности параллельных вычислений в многопроцессорных вычислительных системах с гетерогенной архитектурой

Основным этапом разработанного алгоритма является блок принятия решения о переносе вычислений этапа на графический процессор. Для осуществления сравнения производительности этапа алгоритма на различных

вычислительных устройствах и последующего принятия решения о переносе вычислений используется модифицированная PRAM-модель.

Модифицированная PRAM-модель

В соответствии с моделью специализированного мультипроцессора, которая является общей для всех моделей графических процессоров, сформирован абстрактный вычислительный мультипроцессор. Для абстрактного вычислительного мультипроцессора имеем следующее множество параметров $\{q_{max}, q_{warp}, M_s, S_{GPU}, K\}$, учитывающих основные характеристики реальных специализированных мультипроцессоров. Для разработки параллельного алгоритма под предложенную модель можно воспользоваться методом создания расписания распределения потоков вычислений, который применяется в базовой PRAM модели, учитывая изложенные выше уточнения и дополнения. В этом случае формулу (1) для верхней оценки времени исполнения алгоритма на PRAM машине следует скорректировать. PRAM модель теперь должна быть представлена в виде одного абстрактного вычислительного мультипроцессора, на котором все скалярные процессоры работают пучками по принципу горизонтального параллелизма. Выражение вычисления верхней оценки временной сложности алгоритма принимает вид

$$T_C(N, p) = O\left(\frac{W(N)}{p} \cdot \left\lceil \frac{p}{q_{warp}} \right\rceil + S(N)\right), \quad (2)$$

где p – число потоков алгоритма, предназначенных для обработки N элементов данных, $p<q_{max}$.

Основным объектом исследования является учет операций обращения к глобальной памяти графического процессора. Необходимо ввести дополнительный параметр алгоритма – сложность обращения к глобальной памяти $R(N)$, которой является суммарное количество обращений на чтение и запись из глобальной памяти графического процессора, требуемое для обработки N элементов данных. Данный вид операций должен присутствовать в любом параллельном алгоритме для графических процессоров, который обрабатывает входные данные. Вследствие того, что процессоры работают в режиме SIMD и выполняют команды последовательно пучками по принципу горизонтального параллелизма, то формула верхней оценки времени исполнения параллельного алгоритма на одном абстрактном вычислительном мультипроцессоре принимает вид

$$T_C^{GPU}(N, p) = O\left(\frac{W(N) + R(N)}{p} \cdot \left\lceil \frac{p}{q_{warp}} \right\rceil + S(N)\right). \quad (3)$$

Исходя из выражения (3), более высокая производительность будет у того алгоритма, который будет иметь меньшее количество обращений к SpRAM. Тогда выражение для определения верхней оценки времени исполнения алгоритма на одном абстрактном вычислительном мультипроцессоре имеет вид

$$T_M(N, p) = \frac{W_M(N) + R_M(N) \cdot K}{S_{GPU} \cdot p} \cdot \left\lceil \frac{p}{q_{warp}} \right\rceil, \quad (4)$$

где $W_M(N)$ – количество элементарных операций одного процессора абстрактного вычислительного мультипроцессора в PRAM,

$R_M(N)$ – количество обращений к SpRAM из одного процессора абстрактного вычислительного мультипроцессора в PRAM.

На основании формулы (3) можно записать выражение для верхней оценки времени исполнения этапа алгоритма

$$T_G(N) = \left\lceil \frac{p}{q_{warp}} \right\rceil \cdot T_M(M, p), \tag{5}$$

Для учета передачи данных между оперативной памяти и памятью SpRAM, следует ввести ещё два дополнительных параметра: суммарное количество входных данных этапа алгоритма в байтах N_{HD} и суммарное количество выходных данных этапа алгоритма в байтах N_{DH}. Тогда выражение вычисления общего времени работы этапа алгоритма принимает вид

$$T_{GPU}(N) = \frac{N_{iHD}(N)}{S_{HD}} + T_G(N) + \frac{N_{iDH}(N)}{S_{DH}}, \tag{6}$$

где S_{HD} и S_{DH} – константы скорости передачи данных между RAM и SpRAM (байт/с).

На основе полученной модели показано, что для анализа и сравнения параллельных алгоритмов необходимо использовать следующие параметры алгоритма:

1) суммарная шаговая сложность $S(N)$

$$S(N) = \sum_{i=1}^{B(N)} S_i(N); \tag{7}$$

2) суммарная рабочая сложность $W(N)$

$$W(N) = \sum_{i=1}^{B(N)} W_i(N); \tag{8}$$

3) суммарная сложность обращения к глобальной памяти специализированного вычислительного модуля $R(N)$

$$R(N) = \sum_{i=1}^{B(N)} R_i(N); \tag{9}$$

4) суммарный объём данных, передаваемых между оперативной памятью вычислительной компьютерной системы и глобальной памятью специализированного вычислительного модуля N_{HD} и N_{DH}

$$\begin{aligned} N_{HD}(N) &= \sum_{i=1}^{B(N)} N_{i\ HD}(N) \\ N_{DH}(N) &= \sum_{i=1}^{B(N)} N_{i\ DH}(N) \end{aligned}. \tag{10}$$

С учетом выражений (7)-(10) верхняя оценка времени работы алгоритма на графическом процессоре в среде CPU-GPU вычисляется следующим выражением

$$T_{GPU}(N) = \frac{N_{HD}(N)}{S_{HD}} + \sum_{i=1}^{B(N)} T_{i\,G}(N) + \frac{N_{DH}(N)}{S_{DH}}. \quad (11)$$

При принятии решения о переносе вычислений на GPU, предварительно производится оценка времени выполнения алгоритма на CPU в соответствие с (2) и оценка времени выполнения алгоритма на GPU в соответствие с (10). После этого осуществляется сравнение полученных временных показателей и по результату принимается решение о переносе вычислений.

Экспериментальное исследование разработанного алгоритма

В качестве тестовой задачи, использовалась задача нахождения нулевых битовых векторов, которая решается с применением генетических алгоритмов [5]. При решении указанной задачи основное время работы занимают параллельные вычисления значений функций приспособленности различных особей, операций скрещивания и мутации. Используемый алгоритм ее решения имеет свойства, характерные для многих генетических алгоритмов:

1) представление особи в виде битовой строки;
2) малое число логических операций при вычислении функции приспособленности, выполнении мутации и скрещивания;
3) последовательный доступ к памяти.

Данные свойства позволяют эффективно использовать вычисления на графическом процессоре.

Для проведения экспериментальной оценки эффективности работы алгоритма оптимизации [6, 7] использовалась тестовая компьютерная система следующей конфигурации: центральный процессор Intel Core 2 Quad Q9400 (2.66GHz), ОЗУ 8 Гбайт, графическая карта Nvidia GeForce GTX560 2 Гбайт 336 потоков, операционная система Windows 7 x64**,** компилятор MS Visual Studio 2008 в release режиме.

При исследовании производительности тестовой задачей изменялось количество 32-битных целых чисел в массиве (M) и число параллельных потоков (N) [8, 9].

Исследовалось среднее время t, потраченное на получение нового поколения для различного количества 32-битных целых чисел в массиве и числа параллельных потоков. Исследования проводились с использованием технологий OpenCL и NVIDIA CUDA.

Результаты экспериментальных исследований приведены в таблице 1.

Таблица 1 – Время генерации многопроцессорной системой одного поколения, N =10, значения приведены в мс

Процессор	Кол-во особей в поколении				
	128	1024	10240	102400	1024000
CPU - Q9400	0,38	0,56	2,5	22,2	416,2
CUDA GPU - GTX460	0,08	0,14	1,03	13	237,4

Как видно из результатов экспериментального исследования, применение разработанного алгоритма оптимизации дает рост производительности относительно центрального процессора – в случае применения NVIDIA CUDA время обработки сокращается с 0,38 мс до 0,08 мс для 128 потоков и с 416,2 мс до 237,4 мс для 102400 потоков [10, 11].

Заключение

Таким образом, на основе модифицированной PRAM-модели, разработан алгоритм повышения производительности параллельных вычислений на специализированных вычислительных модулях, который включает в себя алгоритм принятия решения о переносе вычислений на графический процессор.

Методом оценивания производительности были осуществлены сравнительные экспериментальные исследования разработанного алгоритма. Результаты оценивания алгоритма показывают повышение производительности не менее, чем в 2-4 раза в зависимости от числа исследуемых потоков.

Литература

1. Современные проблемы вычислительной математики и математического моделирования. Т. 1: Вычислительная математика / Под ред. Бахвалова Н. С., Воеводина В. В. – М.: Наука, 2005. – 342 с.

2. Graham R. L. Bounds on Multiprocessing Timing Anomalies // SIAM Journal on Applied Mathematics. 1969. Vol. 17. No. 2. C. 416-429.

3. Колпаков А. А. Аспекты оценки увеличения производительности вычислений при распараллеливании процессоров вычислительных систем // Методы и устройства передачи и обработки информации. 2011. № 1 (13). С. 124-127.

4. Колпаков А. А. Теоретическая оценка роста производительности вычислительной системы при использовании нескольких вычислительных устройств // В мире научных открытий. 2012. № 1. С. 206-209.

5. Капустин Д. С. Ржеуцкая С. Ю. Модификация абстрактной модели параллельных вычислений PRAM с учетом существенных особенностей графических процессоров // Естественные и технические науки. 2011. № 5 (55). С. 336-342.

5. Колпаков А. А. Оптимизация генетических алгоритмов при использовании вычислений на графических процессорах на примере задачи нулевых битовых векторов // Информационные системы и технологии. 2013. № 2 (76). С. 22-28.

6. Кропотов Ю. А. Экспериментальные исследования закона распределения вероятности амплитуд сигналов систем передачи речевой информации // Проектирование и технология электронных средств. 2006. Т. 4. С. 37-42.

7. Кропотов Ю. А., Быков А. А. Алгоритм подавления акустических шумов и сосредоточенных помех с формантным распределением полос режекции // Вопросы радиоэлектроники. 2010. Т. 1 № 1. С. 60-65.

8. Кропотов Ю. А. Временной интервал определения закона распределения вероятности амплитуд речевого сигнала // Радиотехника. 2006. № 6. С. 97-98.

9. Ермолаев В. А., Кропотов Ю. А. О корреляционном оценивании параметров моделей акустических эхо-сигналов // Вопросы радиоэлектроники, 2010. Т. 1 № 1. С. 46-50.

10. Кропотов Ю. А., Проскуряков А. Ю., Белов А. А., Колпаков А. А. Модели, алгоритмы системы автоматизированного мониторинга и управления экологической безопасности промышленных производств // Системы управления, связи и безопасности. 2015. № 2. С. 184-197.

11. Кропотов Ю. А., Белов А. А., Проскуряков А. Ю., Колпаков А. А. Методы проектирования телекоммуникационных информационно–управляющих систем аудиообмена в сложной помеховой обстановке // Системы управления, связи и безопасности. 2015. № 2. С. 165-183.

References

1. *Sovremennye problemy vychislitelnoj matematiki i matematicheskogo modelirovaniya. vol. 1, Vychislitelnaya matematika*. [Modern Problems of Computational Mathematics and Mathematical Modelling. Vol. 1, Computational Mathematics]. Moscow, Science, 2005. 342 p. (in Russian).

2. Graham R. L. Bounds on Multiprocessing Timing Anomalies. *SIAM Journal on Applied Mathematics*, 1969, vol. 17, no. 2, pp. 416-429.

3. Kolpakov A. A. Kropotov Y. A. Aspects of the assessment increase performance of computations in parallel processors of the computing system. *Metody i ustroistva peredachi i obrabotki informatsii*, 2011, vol 13, no. 1, pp 124-127 (in Russian).

4. Kolpakov A. A. Theoretical evaluation of growth performance computing systems from the use of multiple computing devices. *V mire nauchnykh otkrytii*, 2012, no. 1, pp. 206-209 (in Russian).

5. Kolpakov A. A. Optimizing the use of genetic algorithms for computing graphics processors for the problem of zero bit vector *Informatsionnye sistemy i tekhnologii*, 2013, vol. 76, no. 2, pp. 22-28 (in Russian).

6. Kropotov Y. A. Experimental study of the law of distribution of probability of amplitudes of signals of systems of transmission of voice information *Proektirovanie i tekhnologiia elektronnykh sredstv*, 2006, vol. 4, pp. 37-42 (in Russian).

7. Kropotov Y. A. Bykov A. A. Algorithm for suppression of acoustic noise and concentrated interference with the distribution of the formant bands of rejection *Voprosy radiojelektroniki*, 2010, vol. 1, no. 1, pp. 60-65 (in Russian).

8. Kropotov Y. A. The Time Interval of a Definition the Regularity Distribution Probability Amplitudes of Speech Signals. *Radiotehnika*, 2006, no. 6, pp. 97-98 (in Russian).

9. Ermolaev V. A., Kropotov Y. A. On the correlation estimation of parameters of models of acoustic echo-signals *Voprosy radiojelektroniki*, 2010, vol. 1, no. 1, pp. 46-50 (in Russian).

10. Kropotov Y. A., Proskuryakov A. Y., Belov A. A., Kolpakov A. A. Models, Algorithms System of Automated Monitoring and Management of Ecological Safety Industrial Plants. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 184-197. Available at: http://journals.intelgr.com/sccs/archive/2015-02/08-Kropotov.pdf (accessed 24 September 2016) (in Russian).

11. Kropotov Y. A., Belov A. A., Proskuryakov A. Y., Kolpakov A. A. Methods of Designing Telecommunication Information and Control Audio Exchange Systems in Difficult Noise Conditions. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 165-183. Available at: http://journals.intelgr.com/sccs/archive/2015-02/07-Kropotov.pdf (accessed 24 September 2016) (in Russian).

Статья поступила 7 сентября 2016 г.

Информация об авторах

Колпаков Александр Анатольевич – кандидат технических наук. Доцент кафедры «Электроники и вычислительной техники». Муромский институт (филиал) «Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: параллельные и распределенные вычислительные системы. Тел.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Кропотов Юрий Анатольевич – доктор технических наук, профессор. Зав. кафедрой «Электроники и вычислительной техники». Муромский институт (филиал) «Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: телекоммуникационные информационно-управляющие системы. Тел.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Проскуряков Александр Юрьевич – кандидат технических наук. Доцент кафедры «Электроники и вычислительной техники». Муромский институт (филиал) ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевич Столетовых». Область научных интересов: телекоммуникационные системы мониторинга и прогнозирования, обработка информации. Тел.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Адрес: Россия, 602264, г. Муром, ул. Орловская, д. 23.

Improving the Performance of Multiprocessor Computer Systems with Heterogeneous Architecture

A. A. Kolpakov, Y. A. Kropotov, A. Y. Proskuryakov

Purpose. *The task of creating a high-performance computing systems based on computer systems is important because the volume of processed information is constantly increasing. This raises the task of developing algorithms to improve the performance of computer systems. The high performance ensured by architectures with additional computational modules or with homogeneous modules on GPUs. The paper*

had offered to develop the algorithm for improving performance of parallel computation in multiprocessor computing systems with heterogeneous architecture. ***The purpose of paper*** *is modification of the PRAM model for the application of graphical processors.* ***Methods.*** *A method of decomposition of the task into stages, the method of making decisions about the transfer calculations on accelerating the processors are used in paper.* ***Novelty.*** *The new PRAM-model takes into account GPUs. Result. The algorithm for increase of performance of parallel computations in multiprocessor computing systems with heterogeneous architecture is developed in paper. This algorithm based on application of graphical processors as specialized computational modules in the heterogeneous multiprocessor computer system. Its use increased productivity not less than 2-4 times depending on the number of streams under study.* ***Practical relevance.*** *The algorithm and the new PRAM-model can be implemented as a software solution for computer system with the CUDA technology.*

Key words: *parallel computing, algorithm of improving computing performance, PRAM-model, heterogeneous computing systems, graphics processors.*

Information about Authors

Alexsandr Anatolievich Kolpakov – Ph.D. of Engineering Sciences. Associate Professor at the Department of Electronics and Computer Science. Murom Institute (branch) of the «Vladimir State University named after Alexander and Nickolay Stoletovs». Field of research: parallel and distributed computing systems. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Yurij Anatolievich Kropotov – Dr. habil. of Engineering Sciences, professor, Head of Chair «Electronics and Computer Science». Murom Institute (branch) of the «Vladimir State University named after Alexander and Nickolay Stoletovs». Field of research: telecommunication information and control systems. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Alexander Jurievich Proskuryakov – Ph.D. of Engineering Sciences, Associate Professor at the Department of Electronics and Computer Science. Murom institute (branch) of the «Vladimir State University named after Alexander and Nickolay Stoletovs». Field of research: telecommunications monitoring and forecasting system, information processing. Ph.: +7 492 347 72 72. E-mail: kaf-eivt@yandex.ru

Address: Russia, 602264, Murom, st. Orlovskaya, h. 23.

УДК 681.5

Графодинамическое моделирование организационно-технических систем на основе триадных агентов

Юдицкий С. А.

Актуальность. *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 назначения агента, его внутренних «ценностей», «убеждений» и приоритетов, а также от складывающейся внешней и внутренней ситуации; действия, направленные на достижение целей; ключевые параметры агента, вектор которых определяет его состояние. Цели, действия и параметры образуют триаду, что отражено в названии «триадный агент». Структуру такого агента образуют взаимодействующие между собой три компоненты, описываемые «нагруженными» (помеченными) логическими выражениями графами (сетями Петри) – соответственно граф целей, граф действий, граф параметров. Ведущим в триаде является граф действий, который переключается в дискретные моменты времени при выполнении логических условий, формируемых внешней средой и/или двумя остальными графами триадной структуры. Результатом переключения графа действий в текущий дискретный момент являются: переход к новому действию и/или изменение некоторых параметров агента и/или коррекция его целей. Таким образом, сам триадный агент, по сути, является сетью с динамическим поведением и позволяет описать широкий класс динамических процессов в организационно-технических системах (ОТС). При этом, сложные ОТС отличаются большим числом параметров, разместить которые на соответствующем графе одного агента с точки зрения обозримости и наглядности модели не представляется возможным. С другой стороны, число целей и действий в ОТС существенно* меньше *числа ее параметров. В связи с этим для обеспечения обозримости и наглядности целесообразно декомпозировать сложную ОТС на несколько параллельно работающих триадных агентов (не более 7-10).* ***Цель статьи*** *заключается в создании графодинамической модели триадного агента (далее, просто агента) и инструментария на ее основе путем решения следующих частных задач. 1) Формализации и анализа графов целей, действий и параметров агента. 2) Формализации и анализа связей между графами в рамках агента. 3) Введения операций над графами агента («графохирургия»). 4) Алгебраического (символьного) представления графов агента с переходом от описания в форме графа к символьному описанию и обратно. 5) Формализации и анализа связей между агентами в рамках многоагентной триадной сети.* ***Научная новизна*** *работы заключается в создании новой триадной ветви агенто-центрического имитационного моделирования ОТС и поддерживающего ее инструментария, позволяющей упростить процедуру моделирования и повысить его наглядность. Кроме того, к элементам новизны работы стоит отнести: исследование механизма функционирования триадной модели агентов; обоснование нового способа преобразования модели агента с помощью «графохирургической» операции; разработку алгебраического представления графов в виде строки символов, компактно описывающей графы большой размерности (язык СЛОГов – Структурное Логическое Описание Графов), и операции над СЛОГами.* ***Практическая значимость*** *работы подтверждается разработанным в Белгородском государственном технологическом университете им. В.Г. Шухова программным продуктом, предназначенным для использования экспертами при имитационном агентном моделировании сетевых структур, и применении этого продукта при решении промышленных задач.*

Ключевые слова: *графодинамика, триадные агенты, триадные сети, целеполагание, логическое управление, взаимовлияние параметров, механизм взаимодействия графов, графохирургия, алгебра графов, язык слогов, операции над слогами, программная поддержка моделирования.*

Введение

В последние десятилетия в развитых странах наблюдается всё возрастающее применение в различных предметных областях сетевых структур и рост интереса к сетевым моделям в управлении. Резко вырос поток публикаций по этой тематике, в том числе на русском языке. Опубликованы работы по общим вопросам теории сетей [1, 2, 3, 4], по сетевым методам принятия решений [5, 6, 7], по теории социальных сетей [8], сетецентрическому управлению в многоагентных системах [9, 10, 11, 12], рассмотрены многочисленные примеры технологических сетей (в газо- и нефтетранспортных системах [13], электроэнергетике, в компьютерных сетях [14] и т.д.).

Сетевая структура определяется как множество автономных функциональных единиц – агентов, которые могут вступать во взаимодействия друг с другом. Эффективность управления поведением сетевой структуры во многом определяется предварительным имитационным моделированием, в ходе которого определяются временные и ресурсные характеристики системы, конфликтные ситуации, «узкие места» и т.д. Целью моделирования является также прогнозирование процессов развития сетевой структуры, с определением её возможных конфигураций и динамики их преобразования. Модель развития («видение будущего») должна работать на дискретной временной шкале и учитывать не только ожидаемые, но и неожиданные (маловероятные) внешние события. Проблема формального описания и моделирования процессов развития сетевых структур проработана еще в недостаточной мере, одной из попыток продвижения на пути к ее решению следует считать и данную работу.

В статье предложена графодинамическая модель триадного агента на базе классической сети Петри [15, 16], дополненной введенными новыми языковыми конструкциями:

- индикатором сравнения численной переменной с другой переменной или с константой;
- индикатором операции преобразования численной переменной;
- индикаторной логической (булевой) функцией;
- индикаторной продукцией ЕСЛИ – ТО;
- индикаторной сетью (сеть Петри с переходами, помеченными индикаторными продукциями);
- моделью триадного агента в виде тройки индикаторных сетей для графов действий, целей, параметров с буферными позициями между переходами разных графов.

Примеры этих конструкций будут даны ниже. Индикаторы являются булевыми переменными, принимающими два значения – истина (1) и ложь (0). Численные переменные выражают лингвистические значения параметров (типа «низкий», «средний», «высокий» и т.д.) в виде числа балов.

1. Графодинамика триадного агента

Для определения триадной модели агента следует:

- сформировать состав и структуру целей, поставленных перед агентом, установить причинно-следственные связи на множестве целей (целеполагание [6, 7, 17]);
- задать состав и порядок выполнения действий (логическое управление [18, 19, 20]);
- выбрать ключевые параметры, характеризующие работу агента, определить взаимовлияния параметров (когнитивный анализ [21, 22, 23]);
- установить связи между целями, действиями и параметрами.

Решение указанных задач относится к тематике графодинамики [24] – направления в системном анализе, оперирующего переменными в форме графов и отношениями, определенными на графах.

1.1. Моделирование целеполагания

На множестве целей, определяющих деятельность агента, введем отношение подчиненности «цель–подцель», где достижение цели является непосредственным следствием достижения подцелей (подцели детализируют цель). Цели, не подчиненные никакой другой цели, назовем *конечными*, а подцели, которым не подчинены другие цели, – *начальными*.

Конечные цели формулируются абстрактно, в общем виде. Последовательность подчиненных целей, вплоть до начальных, дает необходимые уточнения. Если конечных целей несколько, то они достигаются либо в определенной очередности, либо независимо друг от друга.

Целеполагание является предметом интеллектуальной деятельности специалиста, проводящего моделирование. Психология целеполагания с акцентом на допускаемые типовые ошибки, приводящие к неудачам, описаны в [25].

Формальный аппарат целеполагания базируется на индикаторных сетях, позиции которых сопоставлены целям c_i, $i = 1, \ldots, r$, а переходы помечаются индикаторными продукциями. Пример такого графа дан на рис. 1.

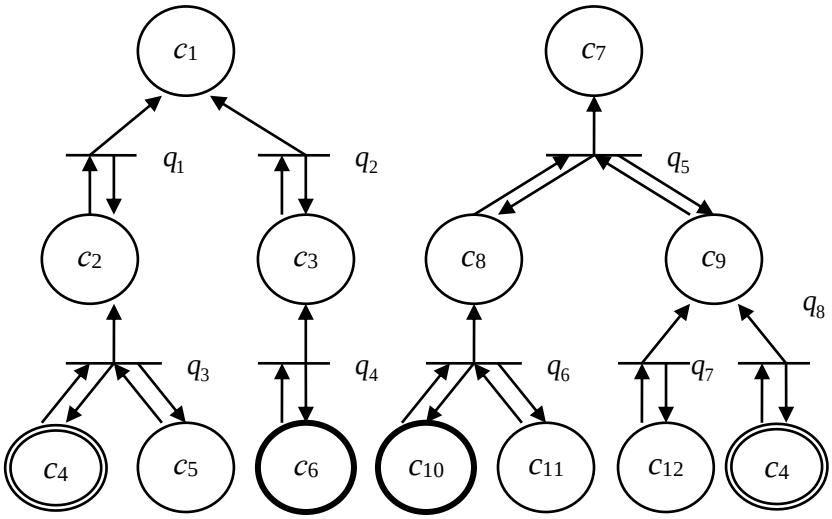


Рис. 1. Пример сети Петри, являющейся основой графа целей

Переходы q_j, $j = 1, \ldots, s$, связывают цель c_i с подчинёнными ей подцелями, где каждая подцель соединена с переходом двумя противоположно направленными стрелками, а переход соединен с каждой своей выходной целью – одной стрелкой. Каждая позиция c_i либо пуста ($c_i = 0$ – цель не достигнута), либо содержит один маркер ($c_i = 1$ – цель достигнута).

Если во всех входных позициях перехода q_j есть по маркеру и все его выходные позиции пусты, и, кроме того, выполняется условие соотнесенной переходу продукции (ее левая часть), то переход срабатывает, вносит маркер в каждую выходную позицию c_i, сохраняя маркирование входных позиций, и выполняет действие (оператор, указанный в правой части продукции). После этого дуга $q_j c_i$ «запирается», что исключает попадание второго маркера в выходную позицию c_i.

Дадим необходимые определения, поясняющие использованную в статье терминологию [26].

Индикатором сравнения – называется булева функция $z=(x\#y)$, принимающая единичное значение, если выполняется отношение #, и нулевое, если не выполняется. Где: x, y – численные переменные, «y» может быть константой, # – знак отношения сравнения из множества $\{=, >, \geq, <, \leq\}$.

Индикаторной логической функцией (ИЛФ) называется выражение, полученное применением конечного числа раз к индикаторам сравнения булевых операций конъюнкции (И), дизъюнкции (ИЛИ) и отрицания (НЕ), изображаемых соответственно ^, v, чертой над символом.

Индикатором преобразования численной переменной $x(\tau)$ при наступлении следующего момента $\tau+1$ называется булева функция $y(\tau+1)=(x(\tau+1)=\Phi(x(\tau)))$, где: Ф – оператор преобразования; $y=1$ в момент $\tau+1$ при выполнении преобразования Ф, и $y=0$ во все остальные моменты.

Индикаторной продукцией называется причинно-следственное выражение вида У→О, где: У – условие, выражаемое индикаторной логической функцией; О – оператор, являющийся следствием, представленный конъюнкцией индикаторов преобразования.

Индикаторной сетью называется сеть Петри с переходами, помеченными индикаторными продукциями.

При работе сетевой модели целеполагания маркеры продвигаются «снизу–вверх» по древовидным графам целей (граф целей – ациклический, любой переход в нем срабатывает не более одного раза). При этом могут использоваться два вида отношения «цель–подцели», при числе подцелей не менее двух: конъюнктивное и альтернативное.

При конъюнктивном отношении обязательно выполнение всех подцелей, которые являются составными частями цели.

При альтернативном отношении необходимо и достаточно выполнение только одной подцели (при недетерминированном выборе этой подцели).

В примере на рис. 1 конъюнктивными являются отношения: $(c_2 – c_4, c_5)$, $(c_7 – c_8, c_9)$, $(c_8 – c_{10}, c_{11})$, а альтернативными: $(c_1 – c_2, c_3)$, $(c_9 – c_4, c_{12})$.

Среди начальных подцелей (позиций) на рис. 1 выделим *противоречивые подцели* (изображаются жирными кружками) и *совпадающие подцели* (изображаются двойными кружками).

Противоречивые начальные позиции c_i, c_j находятся в отношении альтернативности, обеспечиваемом логической функцией $\alpha = \bar{c}_i \wedge \bar{c}_j$ называемой семафором. Маркирование противоречивых позиций возможно только при $\alpha = 1$, что имеет место при пустых позициях. Если первым маркер попадает в одну из противоречивых позиций, например $c_i = 1$, то $\alpha = 0$, и вход в c_j блокируется. Совпадающие позиции являются экземплярами одной и той же начальной подцели. В примере на рис. 1 противоречивы позиции c_6, c_{10} и совпадают две позиции c_4.

Результатом моделирования целеполагания является линейный график достижения целей на заданном временном горизонте $[\tau = 0, \ \tau = N]$, пример которого дан на рис. 2. Интервалы горизонта, на которых цели c_i достигнуты, заштрихованы. График достижения целей строится непосредственно по графу целей.

T	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
c_1									■	■	■	■	■	■	■	■	■	■	■	■	■
c_2								■	■	■	■	■	■	■	■	■	■	■	■	■	■
c_3												■	■	■	■	■	■	■	■	■	■
c_4					■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
c_5							■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
c_6																					
c_7																	■	■	■	■	■
c_8																■	■	■	■	■	■
c_9						■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
c_{10}											■	■	■	■	■	■	■	■	■	■	■
c_{11}															■	■	■	■	■	■	■
c_{12}													■	■	■	■	■	■	■	■	■

Рис. 2. Линейный график достижения целей

В примере на рис. 2 в момент $\tau = 4$ достигаются (вследствие внешнего воздействия) оба экземпляра подцели c_4. Левая подцель не влияет на свою цель c_2, правая вызывает в следующий момент $\tau = 5$ достижение цели c_9. Дальнейших переключений (без воздействия на начальные позиции) не происходит, в графе целей устанавливается равновесие. В момент $\tau = 6$ маркер заносится в начальную позицию c_5, срабатывает переход q_3 и в момент $\tau = 7$ маркер вносится в позицию c_2. Далее в момент $\tau = 8$ срабатывает q_1 и маркер вносится в позицию c_1, достигнута первая конечная цель. Граф целей продолжает функционировать подобным образом. В момент $\tau = 15$ маркеры находятся в позициях c_8, c_9 и выполняется условие $c_1 \wedge \bar{c}_7 = 1 \wedge 1 = 1$. Это приводит к

срабатыванию перехода q_5 и внесению маркера в позицию c_7. Таким образом, достигнута вторая конечная цель c_7, причём строго после первой c_1.

На графике на рис. 2 есть несогласованность (на внимание читателя): строка c_3 не должна быть заштрихована, т.к. начальная цель c_6 не достигнута, и правая цепочка, ведущая в конечную цель c_1, в данном имитационном эксперименте не задействована.

1.2. Моделирование логического управления действиями агента

Для моделирования порядка выполнения действий и обусловленного этим порядком логического управления агентами применяются *графы действий*, называемые также *графами операций* [18].

Пример сети Петри, как основы графа действий, дан на рис. 3. При этом, переходы изображены прямоугольниками, а соответствующие этим переходам индикаторные продукции, которые будут далее рассмотрены отдельно – опущены. Для обоснования разветвлений в описании поведения агента даны воздействия V внешней среды: v_1 и v_2.

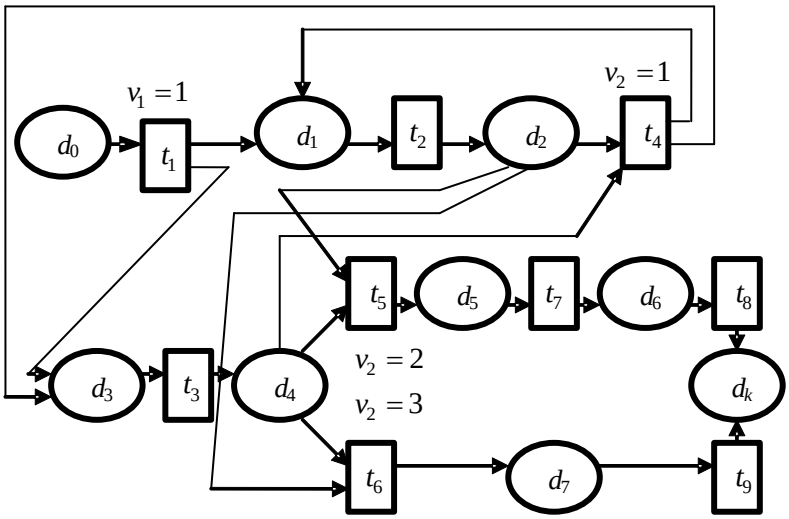


Рис. 3. Сеть Петри как основа графа действий

В любой позиции d_i находится один маркер, если соответствующее действие выполняется, и позиция пуста, если не выполняется. Переход t_j срабатывает мгновенно, если одновременно выполняются следующие условия:

- во всех входных позициях перехода есть по маркеру;
- выполняются соотнесенное переходу внешнее условие v_k и условия, формируемые графами целей и параметров;
- с момента активирования перехода прошло не менее заданного числа единиц модельного времени.

В результате срабатывания перехода из всех его входных позиций удаляются, а во все выходные позиции вносятся маркеры. Временной график логического управления действиями агента является частью итоговой диаграммы моделирования, помещенной на рис. 4.

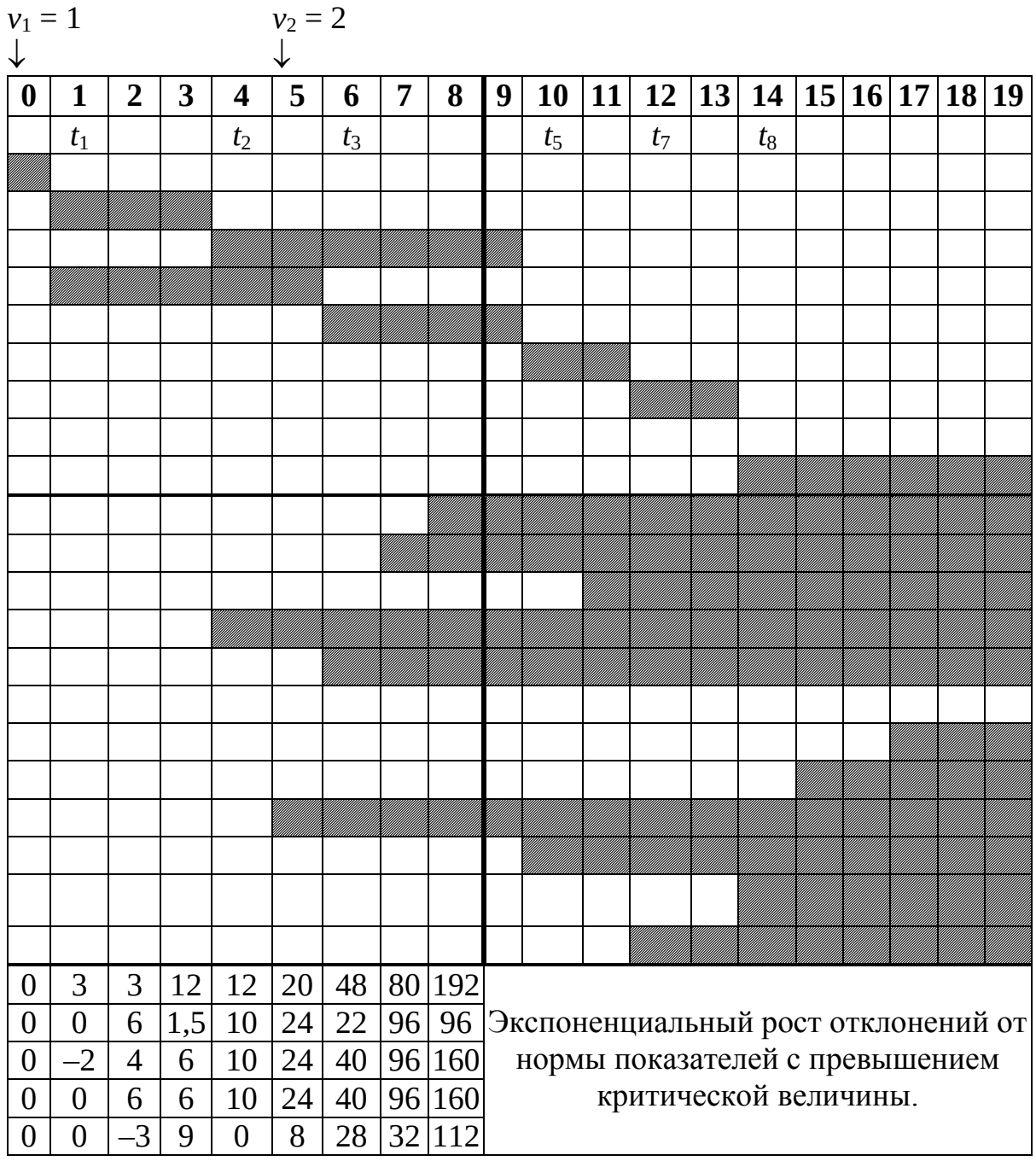


Рис. 4. Итоговая диаграмма моделирования триадной структуры агента

В верхней строке диаграммы указаны моменты времени, образующие горизонт моделирования. В следующей строке проставлены соотнесенные определенному моменту переходы графа действий, в которые происходит смена действий, достижение целей, изменение величины параметров. В верхнем ярусе диаграммы даны линейные графики булевых переменных, сопоставленных действиям (d_0, d_k – начальное и конечное «пустые» действия, обозначающие подготовленность к моделированию и его завершение). В среднем ярусе представлены линейные графики достижения целей, в нижнем дана таблица бальных значений параметров. Вертикальная жирная линия разделяет допустимый и недопустимый интервалы горизонта моделирования.

Итог моделирования поведения агента: при заданной триадной структуре полностью выполняются действия d_1, d_3 и лишь частично d_2, d_4; достигаются цели c_1, c_2, c_4, c_5, c_9; в момент $\tau = 8$ значения параметров p_1, p_3, p_4, p_5 выходят за критическую отметку $p_i^{max}=100$, а отклонение p_2 вплотную приблизилось к ней. Поэтому в момент $\tau = 8$ имитационный эксперимент прекращаем.

1.3. Моделирование взаимовлияния параметров агента

Лингвистическая (словесная) оценка величины параметров, выражаемая числом условных балов, и прогнозы изменения параметров при работе создаваемой системы, выполняются экспертами на предпроектной стадии, и являются достаточно грубыми. Результатом такого предварительного моделирования могут стать тенденции, которые по мнению экспертов проявятся при работе системы. Но для этого надо ввести в модель некоторые гипотетические уточнения.

1. Примем, что параметры агента могут изменяться в моменты, непосредственно следующие за наступлением нового такта (интервала) $\tau = 1, 2, \ldots, N$ на заданной временной шкале, как следствие срабатывания перехода t на графе действий в начальный момент такта τ, а также выполнения условий достижения определенных целей при определенном состоянии внешней среды.

2. Изменение параметров может вызвать изменение других параметров и т.д. с установлением равновесия в том же такте. Процесс изменения описывается графом параметров (рис. 5), а равновесие обеспечивается индикаторными продукциями переходов r_i этого графа.

3. Параметры изменяются на бальной предметной шкале, содержащей, например, 100 пунктов, где каждый 10-й пункт имеет лингвистическую интерпретацию. Эксперты формулируют свои оценки в лингвистических терминах.

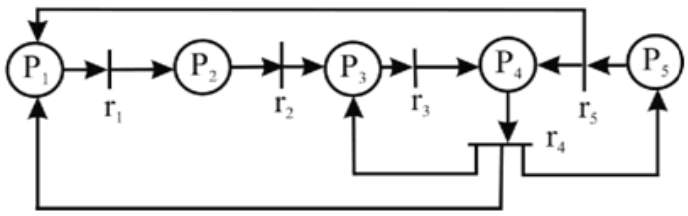


Рис. 5. Сеть Петри как основа графа параметров

Приведем пример бальной предметной шкалы: 0 – без оценки, 10 – очень плохо, 20 – плохо, 30 – между плохо и удовлетворительно, 40 – удовлетворительно, 50 – между удовлетворительно и хорошо, 60 – хорошо, 70 – между хорошо и отлично, 80 – отлично, 90 – между отлично и превосходно, 100 – превосходно.

1.4. Механизм взаимодействия графов действий, целей и параметров при работе агента

Рассмотрим вначале механизм взаимодействия сетей Петри, составляющих основу графов агента, при выполнении описанного выше переходного процесса, инициированного наступлением нового такта в момент τ (рис. 6).

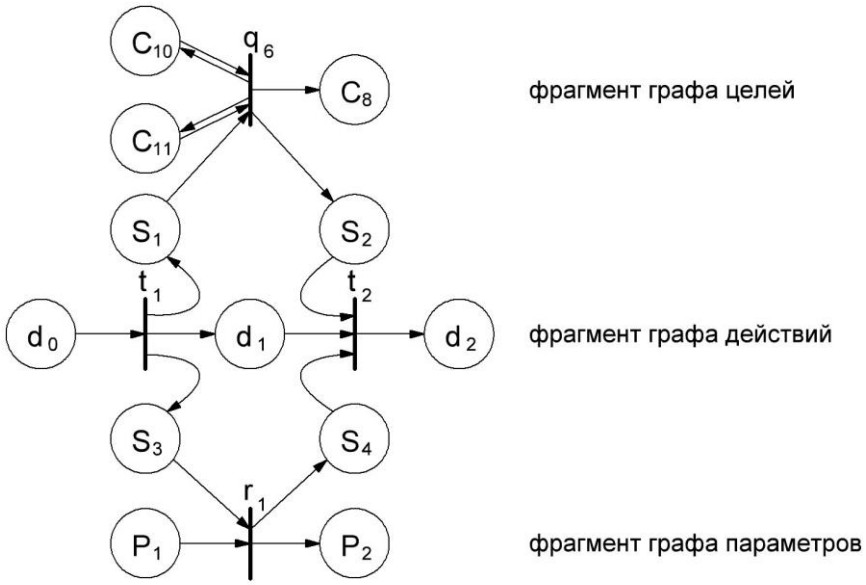


Рис. 6. Механизм взаимодействия графов агента

Каждую из трех сетей будем представлять фрагментом с переходом (переходами), помеченным индикаторной продукцией. Связи между сетями (фрагментами) обеспечиваются введением дополнительных «буферных» позиций s_i и структурой продукций. Буферная позиция принимает только два значения: 1 и 0, т.е. является булевой.

Переходы, срабатывающие в переходном процессе, – t_1, t_2 (граф действий), q_6 (граф целей), r_1 (граф параметров), соотнесены следующим индикаторным продукциям:

$$\Pi(t_1): (d_0(\tau)=1)\wedge(d_1(\tau)=0)\wedge(s_1(\tau)=0)\wedge(s_3(\tau)=0)\wedge(\tau=1) \rightarrow$$
$$\rightarrow (d_0(\tau+1)=0)\wedge(d_1(\tau+1)=1)\wedge(s_1(\tau+1)=1)\wedge(s_3(\tau+1)=1); \quad (1)$$

$$\Pi(t_2): (d_1(\tau)=1)\wedge(d_2(\tau)=0)\wedge(s_2(\tau)=1)\wedge(s_4(\tau)=1)\wedge(\tau=2) \rightarrow$$
$$\rightarrow (d_1(\tau+1)=0)\wedge(d_2(\tau+1)=1)\wedge(s_2(\tau+1)=0)\wedge(s_4(\tau+1)=0); \quad (2)$$

$$\Pi(q_6):(c_8(\tau)=0)\wedge(c_{10}(\tau)=1)\wedge(c_{11}(\tau)=1)\wedge(s_1(\tau)=1)\wedge(s_2(\tau)=0)\wedge(\tau=1)\rightarrow$$
$$\rightarrow(c_{10}(\tau+1)=1)\wedge(c_{11}(\tau+1)=1)\wedge(s_1(\tau+1)=0)\wedge(c_8(\tau+1)=1)\wedge(s_2(\tau+1)=1); \quad (3)$$

$$\Pi(r_1): (p_1(\tau)>20)\wedge(p_1(\tau)<60)\wedge(p_2(\tau)<80)\wedge(s_3(\tau)=1)\wedge(s_4(\tau)=0)\wedge(\tau=1) \rightarrow$$
$$\rightarrow(p_1(\tau+1)=p_1(\tau)-10)\wedge(p_2(\tau+1)=p_2(\tau)+10)\wedge(s_3(\tau+1)=0)\wedge(s_4(\tau+1)=1). \quad (4)$$

Для моделирования взаимодействий между графами агента задаются начальные условия в виде значений переменных – булевых для действий *d*,

целей c, буферных позиций s, и бальные оценки для параметров p, в начальный момент $\tau=0$. Далее, с помощью индикаторных продукций типа (1)–(4) вычисляются значения переменных для последующих тактов $\tau=1, 2, \ldots, N$.

Пусть в начальный момент $\tau=0$: $d_0=1$, $d_1=0$, $d_2=0$, $c_{10}=1$, $c_{11}=1$, $c_8=0$, $p_1 \in [20, 60]$, $p_2=40$, $s_1=s_2=s_3=s_4=0$, ни один переход не активирован.

В момент начала такта $\tau=1$ срабатывает переход t_1, изымающий маркер из d_0 и вносящий маркеры в d_1, s_1, s_3. Это приводит к активированию двух переходов – q_6 и r_1, которые могут сработать в любой последовательности либо одновременно (описываемая структура является расширением классической сети Петри, в которой запрещается одновременное срабатывание двух и более переходов). При срабатывании перехода q_6 маркеры остаются в позициях c_{10} и c_{11} ,обнуляется буферная позиция s_1 и маркеры вносятся в позиции c_8, s_2. При срабатывании перехода r_1 в его входной позиции p_1, значением которой эксперт указал только принадлежность к интервалу на бальной шкале, согласно оператору продукции (4) верхняя и нижняя границы этого интервала уменьшаются на 10, т.е. он принимает вид $p_1=[10, 50]$, а выходные позиции принимают значения $p_2=40+10=50$, $s_4=1$. При установившемся маркировании переменных активируется и срабатывает в следующем такте $\tau=2$ переход t_2, удаляются маркеры из всех его входных позиций, и вносится маркер в выходную позицию d_2. Переходный процесс в структуре на рис. 6 в такте $\tau=1$ завершен, и структура пришла в равновесное состояние.

1.5. Операции над графами – графохирургия

Существует содержательная аналогия между медицинскими хирургическими операциями типа пересадки тканей и органов, «вживления» (имплантации) искусственных устройств – кардиостимуляторов, сердечных клапанов, протезов суставов и т.д., и операциями преобразования графов. При классической медицинской операции последовательно выполняются следующие этапы:

1) разрез тканей и доступ к пораженному органу;
2) «отключение» органа от системы кровообращения (и, возможно, других систем организма);
3) удаление пораженного органа или его части (например, новообразования);
4) при имплантации – «вставка» замещающего органа; сшивание сосудов и тканей.

При выполнении операции преобразования графа будем применять следующий базовый алгоритм.

1. Выделяем (замкнутой пунктирной линией) фрагмент графа, который подлежит замене. Граничные переходы выделенного фрагмента представляем в виде связок – совокупности синхронизированных компонентов перехода, которые по определению срабатывают одновременно, и только одновременно [26, 27] (понятие «связка» вписывается в используемое в работе расширение классических сетей Петри). Каждый компонент связки принадлежит либо выделенному

фрагменту, либо остальной части графа. Таким образом, выделенный фрагмент оказывается отделенным от исходного графа.

2. Удаляем фрагмент, отделенный от остальной части графа.
3. Вставляем новый фрагмент, замещающий удаленный, с формированием связок, синхронизирующих источники нового фрагмента и стоки остальной части графа (источниками и стоками согласно работе [27] названы переходы, которые соответственно не содержат входных или выходных дуг). Замещающий фрагмент может быть «пустым», не содержащим ни одной позиции.
4. Каждую введенную связку заменяем одним переходом («сшивание» компонентов связки).

Ввиду отмеченного выше подобия между медицинскими операциями и операциями преобразования графов последние будем называть *графохирургическими операциями*.

Проиллюстрируем базовый алгоритм проведения графохирургических операций на примерах.

В графе на рис. 7 а выделены два фрагмента: верхний и нижний, содержащие соответственно позиции a_3, a_5 и a_4, a_6. Граничными переходами для этих фрагментов служат b_2, b_7, представимые связками $b_2=\{b_2^1, b_2^2, b_2^3\}$, $b_7=\{b_7^1, b_7^2, b_7^3\}$. Удаляем верхний и нижние фрагменты, выделенные на рис. 7 а верхний черным, а нижний красным пунктиром, и замещаем их фрагментами, показанными на рис. 7 б, – верхним на базе позиций a_8, a_9 и нижним пустым фрагментом. Далее «сшиваем» связки b_2, b_7 и получаем граф, изображенный на рис. 7 в.

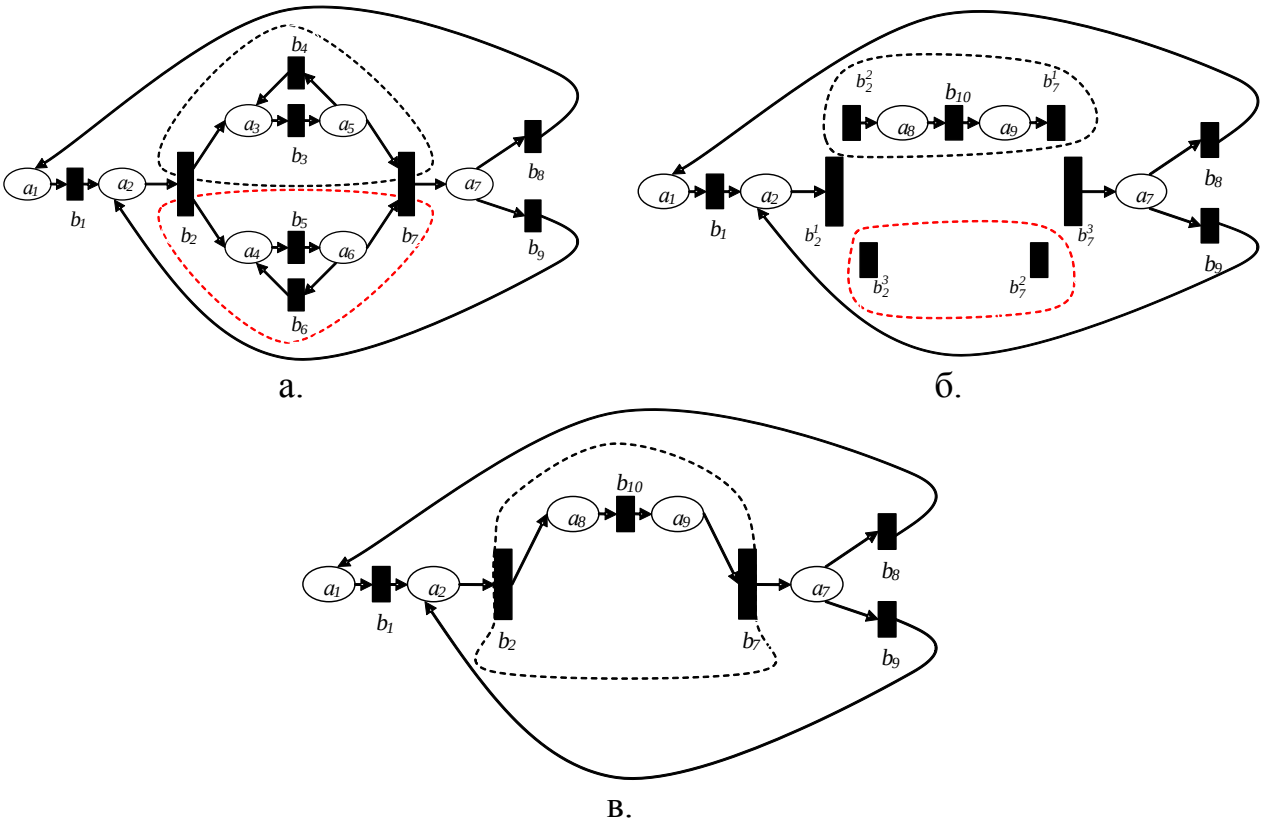


Рис. 7. Пример графохирургической операции

Базовый алгоритм может быть применен для различных вариантов графохирургических операций.

На рис. 8 показана операция совмещения двух позиций графа с заменой их одной позицией. Входными (выходными) переходами совмещенной позиции становятся входные (выходные) переходы совмещаемых позиций. Пусть, например, требуется совместить позиции a_2 и a_7. Выделяем (рис. 8 а) и удаляем позицию a_7 (рис. 8 б) и переходы b_7, b_8, b_9 соединяем дугами с позицией a_2 (рис. 8 в). Из b_7 в a_2 выводится выходная дуга, из a_2 в b_8 и из b_8 в a_1 – также выходные дуги, переход b_9 связан с позицией a_2 входной и выходной дугами.

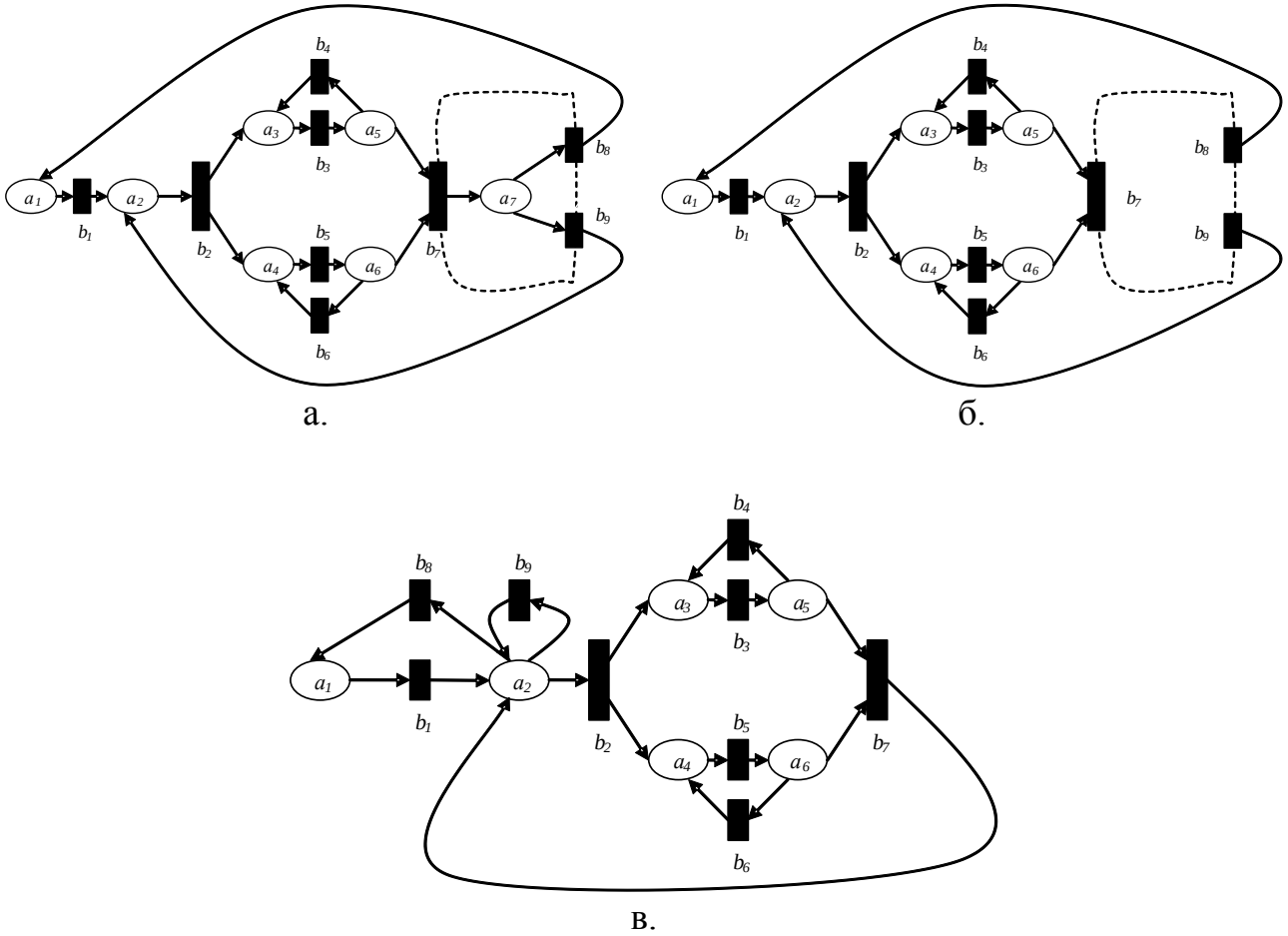
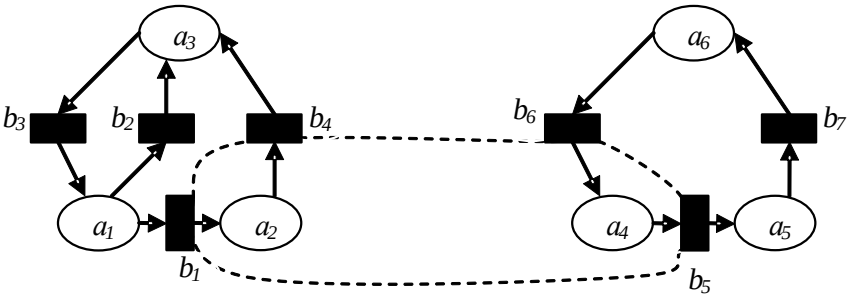


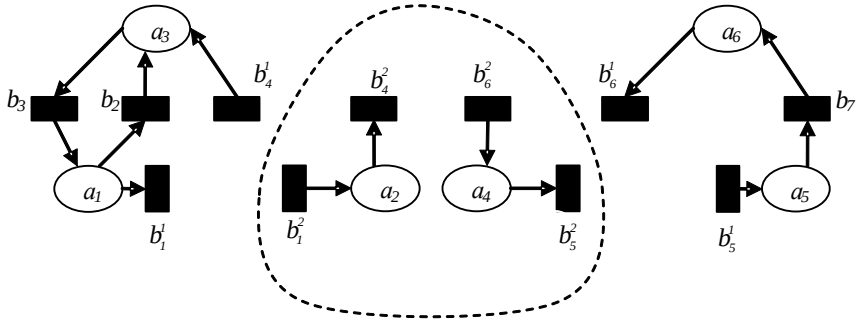
Рис. 8. Пример операции совмещения позиций

На рис. 9 даны примеры преобразования пары графов: соединения их в один граф и введения в графы дополнительных дуг. На рис. 9 а выделен фрагмент, состоящий из позиций a_2, a_4, принадлежащих разным графам. Далее по переходам b_1, b_4, b_5, b_6 вводятся связки и отделяется центральный фрагмент (рис. 9 б). После удаления этого фрагмента, вставки замещающего фрагмента с внутренними переходами b_8, b_9 и «сшивания» соответствующих связок, приходим к единому графу, показанному на рис. 9 в. Другой вариант преобразования графов на рис. 9 а заключается в том, что в оставшихся после удаления центрального фрагмента частях формируются связки, содержащие помимо компонентов «разрезанных» переходов и «неразрезанные» переходы:

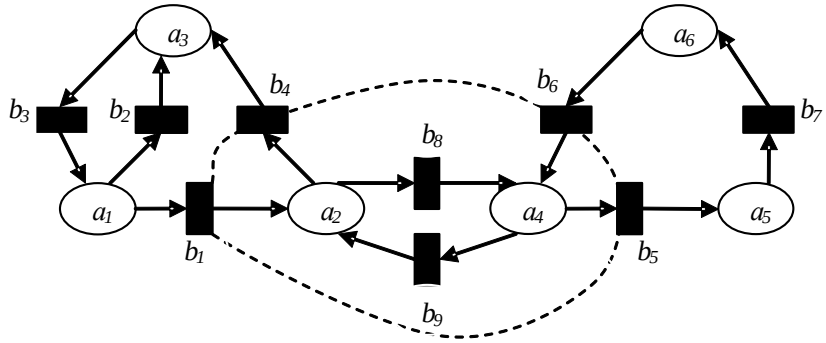
$\{b_1^1, b_3, b_4^1\}$, $\{b_5^1, b_6^1, b_7\}$. После «сшивания» связок получим графы, приведенные на рис. 9 г.



а.

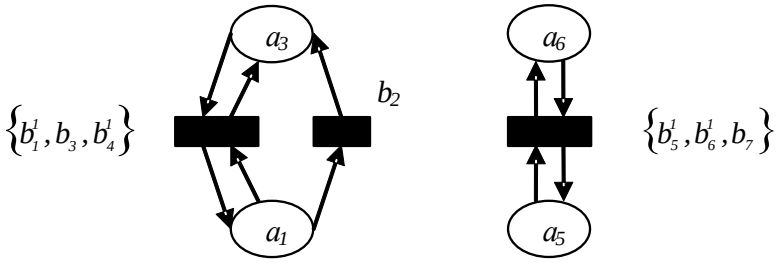


б.



$$b_1 = \{b_1^1, b_1^2\};\quad b_4 = \{b_4^1, b_4^2\};\quad b_5 = \{b_5^1, b_5^2\};\quad b_6 = \{b_6^1, b_6^2\}$$

в.



г.

Рис. 9. Графохирургическое преобразование пары графов:
в – введение соединительного фрагмента; г – введение дополнительных дуг

Управление процессом функционирования сети предусматривает возможность изменения ее структуры – как в части действующих графов, так и

взаимодействий между ними. Известен ряд типовых операций, отображающих преобразование графов: введение/удаление элемента сети (позиции или перехода), слияние позиций, копирование подграфа и т.д. [13, 28, 29]. Список типовых операций является открытым и при необходимости может пополняться.

Таким образом, в этой части работы предложен общий (графохирургический) метод преобразования графов, на основе которого могут порождаться типовые операции (интерпретируемые как частные случаи общего решения). Метод позволяет вносить выборочные изменения в определенные фрагменты системы, сохраняя преемственность в отношении остальной ее части.

Графохирургия включает:

- «разрезание» некоторых переходов сети с формированием так называемых связок – подмножеств синхронизированных переходов;
- отделение и удаление фрагмента сети;
- вставку на его место другого фрагмента; «сшивание» связок – замена их неструктурированными переходами.

1.6. Взаимодействие агентов в многоагентной системе

Многоагентная триадная сеть представляет собой множество взаимосвязанных агентов (субъектов или объектов), в которой [10]:

- каждый агент сохраняет свою индивидуальность, а именно имеет собственные (индивидуальные) цели, выполняет направленные на достижение этих целей индивидуальные действия, характеризуется индивидуальными параметрами;
- связанность агентов заключается в том, что их деятельность может координироваться во времени, и в определенные моменты они могут передавать друг другу сообщения и ресурсы;
- результатом индивидуальной деятельности агентов является достижение определенных коллективных целей и определенная динамика коллективных параметров.

Задача синтеза многоагентной сети в общем виде формулируется следующим образом. Известен набор агентов, представленных, например, триадными структурами, отображающими взаимовлияние графов индивидуальных целей, действий, параметров, и заданы коллективные цели и параметры. Требуется определить, можно ли путем организации связей между агентами создать сеть, в которой наряду с индивидуальными целями достигались бы и желаемые коллективные цели при допустимых значениях индивидуальных и коллективных параметров. Если желаемых целей достичь нельзя, то какие коллективные цели реально достижимы? Аналитическое решение задачи синтеза сети с получением соответствующих необходимых и достаточных условий представляется весьма трудным и может стать предметом специальной работы. В данной статье автор ограничивается построением модели, позволяющей подбирать компоненты многоагентной сети и проверять эффективность такого подбора с помощью имитационного моделирования.

Рассмотрим некоторые аспекты внешнего поведения сети, определяемые взаимодействиями между агентами. Два агента считаются связанными, если их индивидуальная деятельность (как уже говорилось) координируется во времени, и в определенные моменты они могут передавать друг другу информационные или/и материальные ресурсы.

Переходы b_1, b_2, принадлежащие разным агентам и помеченные соответственно продукциями $У_1 \rightarrow О_1$, $У_2 \rightarrow О_2$, где У – логическое условие, О – оператор, будем называть сильно связанными, если они являются компонентами связки $\{b_1, b_2\}$ [27], т.е. срабатывают только одновременно. Сильно связанные переходы помечаются продукциями $У_1 \wedge У_2 \rightarrow О_1$, $У_1 \wedge У_2 \rightarrow О_2$, обеспечивающими их одновременное срабатывание. Оператор агента, передающего порцию ресурса R, уменьшает значение соответствующей переменной на величину этой порции, а оператор принимающего агента, наоборот, увеличивает значение переменной на ту же величину. Бинарное отношение сильной связанности является временным в том смысле, что участвующие в нем агенты могут поменяться ролями, агент может вступить в связку с другим партнером и т.д. Мотивация к таким переменам – разумный баланс между личными и коллективными интересами и целями (знакомо, правда?).

Многоагентная система – это своеобразное «общество», в котором постоянно возникает и разрушается огромное число связок (верхняя граница при N агентах равна C_N^2 – числу сочетаний из N по 2).

Проследить за динамикой связок в системе с большим числом агентов можно только по усредненным показателям. Тем не менее, конкретизируя интересы и цели реальных агентов и зная назначение и стратегию реальной многоагентной системы, при ограниченном числе агентов (не более 10) можно спрогнозировать наиболее вероятные линии развития системы и провести их имитационное моделирование. Однако, этот вопрос выходит за пределы данной статьи.

2. Алгебраическое представление графов

Модель сети характеризуется статической и динамической составляющей, где статическая составляющая представляется в графовой форме, а динамическая – в алгебраической (в виде индикаторных выражений), что делает модель неоднородной. Кроме того, сложность (а тем самым и наглядность) графового описания экспоненциально возрастает при увеличении его размерности. Следовательно, для моделирования статической составляющей имеет смысл применить алгебраическое описание, линейно зависящее от размерности агентов и сети. В статье для этого введен формальный язык СЛОГов (Структурное Линейное Описание Графов), отображающих ориентированный граф в виде строки, составленной из символов вершин (применительно к двудольному графу – из чередующихся символов позиций и переходов) и нумерованных вертикальных стрелок.

2.1. Язык СЛОГов

СЛОГ взаимно однозначно отображает ориентированный граф – вершины, дуги, функцию инциденций. Примем, что вершины обозначаются символами из алфавита $E=\{e_i,\ i=1,\ldots,n\ \}$, где вершина e_i – это позиция или переход. Если из вершины e_i исходят дуги, ведущие в вершины $e_{j1}, e_{j2},\ldots, e_{jk}$, то первая дуга отображается последовательностью $e_i\, e_{j1}$ символов в строке СЛОГа, остальные – упорядоченными парами пронумерованных вертикальных стрелок. Стрелки подразделяются на выходные, направленные вверх, и на входные, направленные вниз. Выходная стрелка проставляется справа от символа e_i , входные стрелки – слева от символов $e_{j2},\ldots,e_{jk}$. Пара стрелок, соответствующая одной дуге, нумеруется одинаковыми верхними индексами. Применительно к дуге $e_i\, e_{j1}$ стрелки, находящиеся между e_i и e_{j1}, во внимание не принимаются. Если таких стрелок несколько, то вначале проставляются подряд все выходные стрелки, а затем подряд все входные стрелки. Справа от терминальной вершины, из которой не исходит ни одной дуги, ставится восклицательный знак – «!».

Алгебраическое представление СЛОГов проиллюстрируем на примере графа, изображенного на рис. 8 а:

$$s_1=\downarrow^7 a_1\ b_1\ \downarrow^8 a_2\ b_2\uparrow^1\downarrow^2\ a_3\ b_3\ a_5\ \uparrow^3 b_4\ \uparrow^2\ !\downarrow^1\downarrow^4 a_4\ b_5\ a_6\uparrow^5 b_6\ \uparrow^4 !\downarrow^3\downarrow^5\ b_7\ a_7\uparrow^6 b_8\uparrow^7 !\ \downarrow^6 b_9\uparrow^8 \qquad (5)$$

Следование буквы b_1 непосредственно за a_1 отображает дугу a_1b_1 на графе на рис. 8 а, a_2 за b_1 – дугу b_1a_2 и т.д. Цепочка чередующихся позиций и переходов в СЛОГе завершается буквой b_6, справа от которой стоит знак «!». Другая цепочка – $b_7a_7b_8$. Пара «выходная стрелка – входная стрелка» с номером 1 отображает дугу b_2a_4, пара стрелок с номером 2 – дугу b_4a_3 и т.д.

В общем случае исходному графу соответствует множество эквивалентных СЛОГов, отличающихся порядком букв в строке, числом и местом расположения вертикальных стрелок. Эквивалентность заключается в том, что полученные на их основе графы изоморфны. Среди СЛОГов может быть выбран оптимальный, например, с наименьшим числом стрелок. Однако здесь такая задача не рассматривается. Номера стрелок в СЛОГе (5) соответствуют следующим дугам графа на рис. 8 а: 1 – b_2a_4, 2 – b_4a_3, 3 – a_5b_7, 4 – b_6a_4, 5 – a_6b_7, 6 – a_7b_9, 7 – b_8a_1, 8 – b_9a_2. Непомеченные цифрами дуги графа отражают последовательность букв в строке СЛОГа в порядке слева направо.

Ввод СЛОГа в компьютер удобно выполнять на основе приема, позволяющего сократить число перенастроек клавиатуры: на первом шаге формируется строка из букв a_i, b_j, на втором шаге расставляются стрелки, на третьем вводятся номера стрелок.

2.2. Операции над СЛОГами

Рассмотрим элементарные операции над СЛОГами, подобные тем, которые выполняются при графохирургических преобразованиях на графах (раздел 1.5 статьи). Алгоритм преобразования СЛОГа состоит из следующих шагов.

1. *Формирование связок синхронизированных переходов* $b_i=\{b_i^1,\ldots,b_i^k\}$, где компоненты связки срабатывают одновременно, и только одновременно. В качестве примера рассмотрим СЛОГ (5), в котором заместим связками переходы b_2 и b_7:

$$s_2=\downarrow^7 a_1\, b_1 \downarrow^8 a_2\ \{b_2^1, b_2^2, b_2^3\}\ \uparrow^1\downarrow^2 a_3\, b_3\, a_5\uparrow^3 b_4\ \uparrow^2!\downarrow^1\downarrow^4 a_4\, b_5\, a_6\ \uparrow^5 b_6\ \uparrow^4!\downarrow^3\downarrow^5$$
$$\{b_7^1, b_7^2, b_7^3\}\ a_7\ \uparrow^6 b_8\ \uparrow^7!\downarrow^6 b_9\uparrow^8 \qquad (6)$$

2. *Преобразование связок.* В связке выделяются компоненты, которые будут играть роль источников и стоков для подСЛОГов, образованных в результате разбиения СЛОГа на части (источники и стоки – это переходы, ведущие в подСЛОГ и из него). Стоки и источники в связке будем разделять косой чертой, слева от которой помещаются стоки, а справа – источники. Если непосредственно перед открывающей фигурной скобкой связки (после закрывающей скобки) проставлены входные (выходные) стрелки, то эти стрелки переносятся внутрь скобок, соответственно перед стоками или после источников. В СЛОГе (6) в первой по порядку связке переход b_2^1 объявляем стоком, а b_2^2, b_2^3 – источниками. Стрелку $\uparrow^1$ помещаем внутрь скобок после источника b_2^3, за источником b_2^2 следует буква a_3, помещенная в строке СЛОГа справа от закрывающей скобки связки. Во второй связке перед открывающей скобкой проставлены входные стрелки $\downarrow^3$, $\downarrow^5$, которые помещаем внутри скобок перед стоками b_7^2, b_7^3. Источник b_7^1 не имеет предшественника. В итоге получаем СЛОГ:

$$s_3 = \downarrow^7 a_1\, b_1 \downarrow^8 a_2\ \{b_2^1/b_2^2\, b_2^3\uparrow^1\}\ \downarrow^2 a_3\, b_3\, a_5\ \uparrow^3 b_4\ \uparrow^2!\downarrow^1\downarrow^4 a_4\, b_5\, a_6\ \uparrow^5 b_6\uparrow^4!$$
$$\{\downarrow^3 b_7^2\ \downarrow^5 b_7^3/b_7^1\}\ a_7\uparrow^6 b_8\uparrow^7!\ \downarrow^6 b_9\ \uparrow^8 \qquad (7)$$

3. *Разбиение СЛОГа на подСЛОГи.* ПодСЛОГи выделяются из СЛОГа на основе следующего алгоритма. В СЛОГе фиксируются начальный и конечный символы, которые могут быть как буквой, так и стрелкой. В первом подСЛОГе к начальному символу СЛОГа справа приписывается следующий символ. Если он является стоком данного подСЛОГа или конечным символом СЛОГа, то формирование подСЛОГа завершается. В противном случае приписывается следующий символ, и процедура повторяется. Для последующих подСЛОГов применяется тот же алгоритм с использованием в качестве начального символа соответствующего источника.

Например, для СЛОГа (7) получаем четыре подСЛОГа:

$$s_4^1=\downarrow^7 a_1\, b_1 \downarrow^8 a_2\, b_2^1$$
$$s_4^2= b_2^2\downarrow^2 a_3\, b_3\, a_5\ \uparrow^3 b_4\ \uparrow^2!\downarrow^3 b_7^2$$
$$s_4^3 = b_2^3\ \uparrow^1\downarrow^1\downarrow^4 a_4\, b_5\, a_6\ \uparrow^5 b_6\ \uparrow^4!\downarrow^5 b_7^3$$
$$s_4^4 = b_7^1 a_7\uparrow^6 b_8\ \uparrow^7!\downarrow^6 b_9\ \uparrow^8 \qquad (8)$$

Заметим, что подСЛОГи s_4^2, s_4^3 являются замкнутыми, т.к. все стрелки ведут в тот же подСЛОГ. Для s_4^1, s_4^4 это не так, последний подСЛОГ взаимодействует с первым по стрелкам 7 и 8. Пара расположенных рядом стрелок с номером 1 в третьем подСЛОГе, полученная формально по алгоритму, является излишней и может быть удалена.

4. *Удаление и вставка подСЛОГов.* В наборе подСЛОГов (8) удаляем s_4^2 и замещаем его подСЛОГом $s_4^5=b_{10}\, a_8\, b_{11} a_9\, b_{12}$ с введением связок $b_{13}=\{b_2^1/b_{10}\, b_2^3\}$, $b_{14}=\{b_{12}\ b_7^3/b_7^1\}$, где b_2^1, b_{12}, b_7^3 – стоки подСЛОГов s_4^1, s_4^5, s_4^3, *а* b_{10}, b_2^3, b_7^1 –

источники подСЛОГов s_4^5, s_4^3, s_4^4 соответственно. В результате получаем преобразованный СЛОГ, дополненный указанными выше связками:

$$s_5=\downarrow^7 a_1\ b_1\ \downarrow^8 a_2\ \{b_2^1/b_{10}\ b_2^3\uparrow^9\}\ a_8\ b_{11}\ a_9\ \uparrow^{10}\downarrow^9\downarrow^4\ a_4\ b_5\ a_6\ \uparrow^5 b_6\ \uparrow^4!\downarrow^5 \{\downarrow^{10} b_{12}\ b_7^3/b_7^1\}\ a_7\ \uparrow^6 b_8\ \uparrow^7!\downarrow^6 b_9\ \uparrow^8 \quad (9)$$

5. *«Сшивание» связок и замещение их одним переходом.* В описываемом примере СЛОГ (9) преобразуется в СЛОГ (10), для которого очевидным образом может быть построен граф с неструктурированными переходами.

$$s_6=\downarrow^7 a_1\ b_1\ \downarrow^8 a_2\ b_{13}\ \uparrow^9 a_8\ b_{11}\ a_9\ \uparrow^{10}!\downarrow^9\downarrow^4 a_4\ b_5\ a_6\ \uparrow^5 b_6\ \uparrow^4!\downarrow^5\downarrow^{10} b_{14}\ a_7\ \uparrow^6 b_8\ \uparrow^7!\downarrow^6 b_9\ \uparrow^8 \quad (10)$$

Моделирование развития триадных сетей происходит в тесном взаимодействии человеческого и компьютерного факторов. Рутинные задачи выполняются компьютерами, а творческие, в первую очередь принятие решений, решаются человеком. Чем в большей степени автоматизирован процесс моделирования, т.е. чем существеннее «компьютерная доля», тем больше возможностей имеет человек для решения творческих прорывных задач. В этом контексте описанный в статье графохирургический подход к преобразованию триадных сетей, базирующийся на элементарных операциях введения связок переходов, «разрезания» связок, удаления и вставки фрагментов сети, «сшивания» связок и т.д., конструктивно поддержанный алгеброй СЛОГов, может способствовать повышению уровня автоматизации моделирования триадных сетей.

3. Программная поддержка моделирования триадных сетей

Для повышения уровня автоматизации моделирования триадных сетей было разработано специальное программное обеспечение для их интерактивного имитационного моделирования. Данное программное обеспечение разработано А.В. Чуевым под руководством проф. В.З. Магергута и при участии научного консультанта разработки проф. С.А. Юдицкого. Описание функциональности этого программного обеспечение представлено в работах [30, 31].

Заключение

Предполагается, что автоматизированная система имитационного моделирования нужна для анализа поведения моделируемой сетевой структуры (в т.ч. определения временных и ресурсных характеристик, конфликтных ситуаций, «узких мест» и т.д.) и прогнозирования процессов развития моделируемой сетевой структуры, с определением её возможных конфигураций и динамики их преобразования. Это нужно для того, чтобы ЛПМ (Лицо, Проводящее Моделирование) могло понять динамику выбранной сетевой структуры, оказать на нее управляющие воздействия и изменить направление ее развития.

Имитационное моделирование процесса развития сетевой структуры реализуется в форме диалога введенной модели с ЛПМ согласно следующей схеме:

1) на каждом временном интервале ЛПМ контролирует функционирование модели и фиксирует полученные данные: о достижении целей, о тенденциях изменения параметров, о месте и времени нарушений, например, выходе параметров за допустимые пределы, о преобразованиях графов (на основе базовой операции «замещение фрагмента графа»), установлении в сети непредусмотренных циклов и т.д.;

2) ЛПМ анализирует эти данные и принимает решение о моменте следующего изменения модели и необходимых преобразованиях графов (на основе базовой хирургической операции замещения фрагмента графа).

Вышеупомянутые предположения дают возможность сформировать требования к возможностям автоматизированной системы имитационного моделирования триадных (и бинарных) сетей. Общее требование состоит в проведении при помощи автоматизированной системы *управляемых и воспроизводимых имитационных экспериментов*. На практике требование сводится к выбору того или иного вида имитационного моделирования (в нашем случае выбрано агентное моделирование). Перечислим концептуальные требования.

1. Адекватное представление выбранной моделируемой сетевой структуры и внешней по отношению к ней среды.
2. Реактивная архитектура агента, при которой агент управляет своим поведением, определяя текущую ситуацию, при заданных целях и способах их достижения.
3. Управление жизненным циклом агентов предполагает, в частности, создание, инициализацию, взаимодействие и уничтожение агентов.
4. Оповещение ЛПМ о нарушениях в функционировании моделируемой сетевой структуры.
5. Обеспечение анализа сетевой структуры как на уровне всей сети в целом, так и на уровне отдельно взятого агента. Предполагается расчет параметров как сети, так и агентов. Более того, представляет интерес анализ динамики значений параметров с использованием методов статистического анализа и методов анализа сетей.
6. Обеспечение интерактивного взаимодействия с ЛПМ. ЛПМ должен иметь возможность не только исследовать результаты имитационного моделирования, но и иметь возможность во время выполнения имитационного моделирования изменять параметры как агента (управлять целями, действиями и параметрами), так и сети в целом (например, управлять внешними событиями).
7. Визуализация основных показателей и формирование отчетов по результатам анализа.

Литература

1. Адизес И. Как преодолеть кризисы менеджмента? – М.: Юнити, 2005. – 189 с.

2. Блюмин С. Л. Оргиперграфы: матричное представление // Управление большими системами, 2010, № 30.1. С. 22-39.

3. Воронин А. А., Губко М. В., Мишин С. П., Новиков Д. А. Математические модели организаций. – М.: Ленанд, 2008. – 359 с.

4. Кульба В. В., Кононов Д. А., Чернов И. В., Рощин П. Е., Шулигина О. А. Сценарное исследование сложных систем: анализ методов группового управления // Управление большими системами. 2010. № 30.1. С. 154-186.

5. Бурков В. Н., Буркова И. В. Метод сетевого программирования в задачах управления проектами // Управление большими системами. 2010. № 30.1. С. 40-61.

6. Ларичев О. И. Теория и методы принятия решений, а также хроника событий в Волшебных Странах. – М.: Логос, 2000. 296 с.

7. Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. 278 с.

8. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. – М.: Физматлит, 2010. – 244 с.

9. Амбарцумян А. А. Сетецентрическое управление на сетях Петри в структурированной дискретно-событийной системе // Управление большими системами. 2010. № 30.1. С. 506-535.

10. Городецкий В. И., Грушинский М. С., Хабалов А. В. Многоагентные системы (обзор) // Новости искусственного интеллекта. 1998. № 2. С. 64-116.

11. Затуливетер Ю. С., Фищенко Е. А. Графодинамические системы с сетецентрическим управлением в математически однородном поле компьютерной информации // Управление большими системами. 2010. № 30.1. С. 567-604.

12. Юдицкий С. А., Владиславлев П. Н., Точ Д. С. Триадный подход к моделированию систем сетецентрического управления // Управление большими системами. 2010. № 28. С. 24-39.

13. Анишев П. А. Редуцируемость сетей Петри // Программирование. 1982. №4. С. 36-43.

14. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. – М.: Эдиториал УРСС, 2002. 352 с.

15. Питерсон Дж. Теория сетей Петри и моделирование систем. – М.: Мир, 1984. – 265 с.

16. Котов В. Е. Сети Петри. – М.: Наука, 1984. – 160 с.

17. Юдицкий С. А., Владиславлев П. Н. Основы предпроектного анализа организационных систем. – М.: Финансы и статистика, 2005. – 144 с.

18. Юдицкий С. А., Магергут В. З. Логическое управление дискретными процессами. – М.: Машиностроение, 1987. – 176 с.

19. Марк Г., МакГоуэн К. Методология структурного анализа и проектирования. – М.: МетаТехнология, 1993. – 231 с.

20. Закревский А. Д. Параллельные алгоритмы логического управления. – М.: Едиториал УРСС, 2003. – 200 с.

21. Кузнецов О. П., Кулинич А. А., Марковский А. В. Анализ влияний при управлении слабоструктурированными ситуациями на основе когнитивных карт // Человеческий фактор в управлении. – М.: КомКнига, 2006. С. 313-344.

22. Максимов В. И. Структурно-целевой анализ развития социально-экономических ситуаций // Проблемы управления. 2005. № 3. С. 30-38.

23. Робертс Ф. С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. – М.: Наука, 1986. - 496 с.

24. Айзерман М. А., Гусев Л. А., Петров С. В., Смирнова И. Н. Динамический подход к анализу структур, описываемых графами (основы графодинамики) // Автоматика и телемеханика. 1977. № 7. С. 135-151.; № 9. С. 123-136.

25. Дернер Д. Логика неудачи. – М.: Смысл, 1997. – 236 с.

26. Юдицкий С. А. Моделирование динамики многоагентных триадных сетей. – М.: Синтег, 2012. – 112 с.

27. Таль А. А., Юдицкий С. А. Иерархия и параллелизм в сетях Петри I, II // Автоматика и телемеханика. 1982. № 7. С. 113-122; № 9. С. 83-88.

28. Семенов А. С. Фрактальные развивающиеся архитектуры // Управление большими системами. 2010. № 30.1. С. 91-103.

29. Юдицкий С. А. Графодинамическое имитационное моделирование развития сетевых структур // Управление большими системами. 2011. № 33. С. 21-34.

30. Юдицкий С. А., Магергут В. З., Чуев А. В. Бинарные сетевые дорожные карты процессов управления проектами // Приборы и системы. Управление, контроль, диагностика. 2013. № 4. С. 1-9.

31. Юдицкий С. А., Магергут В. З., Чуев А. В. Программно-алгоритмическое обеспечение моделирования процессов на бинарных индикаторных сетях // Приборы и системы. Управление, контроль, диагностика. 2014. № 9. С. 10-17.

References

1. Adizes I. *Kak preodolet' krizisy menedzhmenta?* [How to Solve the Mismanagement Crisis]. Moscow, Iuniti Pabl., 2005. 189 p. (in Russian).

2. Blumin S. L. Dihypergraphs: Matrix Representations. *Large-scale Systems Control*, 2010, no. 30.1, pp. 22-39 (in Russian).

3. Voronin A. A., Gubko M. V., Mishin S. P., Novikov D. A. *Matematicheskie Modeli Organizatsii* [Mathematical Models of Organizations]. Moscow, Lenand Pabl., 2008, 359 p. (in Russian).

4. Kulba V. V., Kononov D. A., Chernov I. V., Roshchin P. E., Shuligina O. A. Scenario-Based Research of Complex Systems: Analysis of Group Management Methods. *Large-scale Systems Control*, 2010, no. 30.1, pp. 154-186 (in Russian).

5. Burkov V. N., Burkova I. V. Network Programming in Project Management. *Large-scale Systems Control*, 2010, no. 30.1, pp. 40-61 (in Russian).

6. Larichev O. I. *Teoriia i metody priniatiia reshenii, a takzhe khronika sobytii v Volshebnykh Stranakh* [Theory and Methods of Decision-Making, and Also Chronicle of Events in Magic Countries]. Moscow, Logos Pabl., 296 p. (in Russian).

7. Saati T. *Priniatie reshenii. Metod analiza ierarkhii* [Decision-Making. Method of Analysis of Hierarchies]. Moscow, Radio i Sviaz Pabl., 1993. 278 p. (in Russian).

8. 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, Izdatelsvo fiziko-matematicheskoi literatury, 2010. 228 p. (in Russian).

9. Ambartsumyan A. A. Network-Centric Control on Petri Nets for Structured Discrete Event System. *Large-scale Systems Control*, 2010, no. 30.1, pp. 506-535 (in Russian).

10. Gorodetskii V. I., Grushinskii M. S., Khabalov A. V. Mnogoagentnye sistemy (obzor) [Multi-Agent System (Review)]. *Novosti iskusstvennogo intellekta*, 1998, no. 2, pp. 64-116 (in Russian).

11. Zatuliveter Yu. S., Fischenko E. A. Graph-Dynamics Systems with Network-Centric Control in Mathematically Uniform Field of Computer Information. *Large-scale Systems Contro*l, 2010, no. 30.1, pp. 567-604 (in Russian).

12. Yuditskiy S. A., Vladislavlev P. N., Toch D. S. A Triad Approach to Network-Centric Control Systems Modelling. *Large-scale Systems Contro*l, 2010, no. 28, pp. 24-39 (in Russian).

13. Anishev P. A. Redutsiruemost' setei Petri [Reducyruet Petri Nets]. *Programming and Computer Software*, 1982, no. 4, pp. 36-43 (in Russian).

14. Tarasov V. B. Ot mnogoagentnykh sistem k intellektual'nym organizatsiiam: filosofiia, psikhologiia, informatika [From Multiagent Systems to Intellectual Organizations: Philosophy, Psychology, Computer Science]. Moscow, Editorial URSS Pabl., 2002. 352 p. (in Russian).

15. Peterson James L. *Petri net theory and the modeling of systems.* The University of Texas at Austin, 1981.

16. Kotov V. E. *Seti Petri* [Petri Nets]. Moscow, Nauka Publ, 1984, 160 p. (in Russian).

17. Yuditskiy S. A., Vladislavlev P. N. *Osnovy predproektnogo analiza organizatsionnykh system* [The Basics of Pre-Analysis of Organizational Systems]. Moscow, Finansy i Statistika Pupl., 2005, 144 p. (in Russian).

18. Yuditskiy S. A., Magergut V. Z. *The logical control of discrete processes. Model, Analysis, synthesis*. Moscow, Mashinostroyeniye Publ., 1987. 176 p. (in Russian).

19. Mark G., MakGouen K. *Metodologiia strukturnogo analiza i proektirovaniia* [The Methodology of Structural Analysis and Designing]. Moscow, Metatekhnologiia Publ., 1993. 231 p. (in Russian).

20. Zakrevskii A. D. *Parallel'nye algoritmy logicheskogo upravleniia* [Parallel Algorithms of Logical Control].Editorial URSS Publ., 2003. 200 p. (in Russian).

21. Kuznetsov O. P., Kulinich A.. A., Markovskii A. V. Analiz vliianii pri upravlenii slabostrukturirovannymi situatsiiami na osnove kognitivnykh kart

[Analysis of Effects in the Management of Semi-structured Situations Based on Cognitive Maps]. *Chelovecheskii faktor v upravlenii* [The Human Factor in Management], Moscow, KomKniga Publ., 2006, pp. 313-344 (in Russian).

22. Maximov V. I. The Structurally-Objective Analysis of Socio-Economic Situations Development. *Control Sciences*, 2005, no. 3, pp. 30-38 (in Russian).

23. Roberts F. S. Diskretnye matematicheskie modeli s prilozheniiami k sotsial'nym, biologicheskim i ekologicheskim zadacham [Discrete Mathematical Models with Applications to Social, Biological and Environmental Problems]. Moscow, Nauka Publ., 1986. 496 p. (in Russian).

24. Aizerman M. A., Gusev L. A., Petrov S. V., Smirnova I. N. A Dynamic Approach to Analysis of Structures Represented as Graphs (Fundamentals of Graph Dynamics) *Automation and Remote Control*, 1977, no. 7, pp. 135-151; no. 9, pp. 123-136 (in Russian).

25. Derner D. *Logika neudachi* [The logic of failure]. Moscow, Smysl Pabl., 1997. 236 p. (in Russian).

26. Yuditskiy S. A. *Modelirovanie dinamiki mnogoagentnyh triadnyh setej* [Modeling the dynamics of multi-agent triad networks]. Moscow, SINTEG Publ., 2012, 112 p. (in Russian).

27. Tal' A. A., Yuditskiy S. A. Hierarch and Parallelism Petri Nets. *Automation and Remote Control*, 1982, no. 7, pp. 113-122; no. 9, pp. 83-88 (in Russian).

28. Semenov A. S. Fractal Evolutionary Architectures. *Large-scale Systems Control*, 2010, no. 30.1, pp. 91-103 (in Russian).

29. Yuditskiy S. A. Graphodynamic Simulation Modeling of Network Structures Evolution. *Large-scale Systems Control*, 2011, no. 33, pp. 21-34 (in Russian).

30. Yuditskiy S. A., Magergut V. Z., Chuev A. V. Binary network roadmaps project management processes. *Instruments and Systems: Monitoring, Control, and Diagnostics*, 2013, vol. 4, pp. 1-9 (in Russian).

31. Yuditskiy S. A., Magergut V. Z., Chuev A. V. Software for Modeling Processes in Binary Indicator Networks. *Instruments and Systems: Monitoring, Control, and Diagnostics*, 2014, vol. 9, pp. 10-17 (in Russian).

Статья поступила 5 сентября 2016 г.

Информация об авторе

Юдицкий Семен Абрамович – доктор технических наук, профессор, главный научный сотрудник. Институт проблем управления имени В.А. Трапезникова Российской академии наук. Область научных интересов: системный анализ, логическое моделирование, организационно-технологические системы. E–mail: yuseab32@yandex.ru

Адрес: 117321, Москва, Профсоюзная ул. 132, кор. 8, Московский дом-пансионат ветеранов науки, ком. 305.

Graf-Dynamic Modeling of Organizational-Technical Systems Based on the Triad Agents

S. A. Yuditskiy

Relevance. *The network structures are the interacting agents that widely used in various subject areas. Agent behavior is determined by several key factors: the goal of the agent; its priorities; the external and internal situation; the actions to achieve the objectives; the main parameters of the agent, which determine its state. Goals, actions and parameters form a triad – «the triad agent». The structure of this agent has three subsystems, which are formalized based on the theory of Petri nets – the purposes graph, the actions graph and the parameters graph. The main graph is the action graph, which switches in discrete moments of time when certain logical conditions are satisfied. If the action graph takes switching then there is activation of a new action. This action may be the transition to a new action, or changing of the agent settings or changing of the agent goals. Thus, the triad agent is network with dynamic behavior, which allows describing a wide class of dynamic processes in organizational-technical systems. Thus the complex organizational-technical systems are characterized by a large number of parameters that are difficult to place in a graph of a single agent. However, the number of goals and actions in the organizational-technical system is substantially less than the number of its parameters. Thus, complex organizational-technical system, it is advisable to decompose into several parallel functioning triad agents (not more than 7-10). This decomposition ensures the visibility of the model.* ***The purpose of this paper*** *is creating the graf-dynamic model of the triad agents and methods of its research. This is achieved by the solution of the following subtasks. 1) Formalization and analysis of the goals graph, of the actions graph and the agent settings. 2) Formalization and analysis of the relations between the graphs in the agent. 3) Introduction of operations on the agent graphs (the "graph-surgery"). 4) Algebraic (symbolic) graph representation of the agent with the transition from a description in the form of a graph to a symbolic description and back. 5) Formalization and analysis of the relations between agents within the multi-agent triad network.* ***Scientific novelty of the paper*** *is the creation of a new way of building models of organizational-technical system that will simplify its simulation and improve its visibility. In addition, the elements of novelty of the paper include: the research of the mechanism functioning of the triad agents; the rationale of the new method of converting the agent as the "graph-surgery"; the development of an algebraic graph representation as a line of characters (the language of structured Logical Descriptions of Graphs), and operations on them.* ***Practical relevance of the paper*** *is the modeling principles which is used in the software that developed in the Belgorod state technological University n. a. V. G. Shukhov. This software is intended for use by experts for simulation-agent modeling of network structures, and for using at industrial applications.*

Key words: *Graf-dynamic model, triad agent, triad agents net, goal setting, logical control, interference parameters, the mechanism of interaction graphs, graph-surgery, algebra of graphs, language structured Logical Descriptions of Graphs, software support simulation.*

Information about Author

Semen Abramovich Yuditskiy – Dr. habil. of Engineering Sciences, Professor. Chief Researcher. V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. Field of research: system analysis, logic modeling, organizational and technological systems. E–mail: yuseab32@yandex.ru

Address: Russia, 117321, Moscow, Profsoyuznaya street, 132, Bld. 8, Ft. 305, Moscow Pension House of Science Veterans.

УДК 004.052.32

Научно обоснованные предложения по диагностированию распределенной радиотехнической системы наблюдения с множеством технических состояний

Аминев Д. А., Журков А. П., Кроткова К. Г., Охломенко И. В.

Постановка задачи: *радиолокация и радиопеленгация, а, соответственно, и распределенная радиотехническая система наблюдения (РСН) и автоматические радиопеленгаторы (АРП) имеют в настоящее время широкое применение. Так как в удаленных и малоосвоенных районах они являются одним из основных средств обеспечения полетов, то к надежности их работы предъявляются высокие требования. Для обеспечения требований по надежности необходимо осуществлять ее диагностирование. Существующие диагностические методы позволяют определять техническое состояние (ТС) по бинарному критерию, что не подходит к распределенной РСН, имеющей множество ТС ввиду своей пространственной распределенности, сложной иерархии и многомодульности. Поэтому* ***целью работы*** *является формирование подходов к диагностированию распределенной радиотехнической системы с множеством ТС на различных уровнях ее иерархии. Вмесие с тем математически описать способы определения интегральных критериев ТС.* ***Результат:*** *рассмотрена распределенная на местности РСН и состав ее аппаратуры. Приводится классический принцип ее диагностирования по двум техническим состояниям – работоспособное и неработоспособное. Предложены новые подходы на основе известных математических принципов для диагностирования распределенной РСН по множеству технических состояний. Варианты определения итогового ТС: методом наихудшего случая, методом усредненных диапазонов, методом с заданием приоритетов. Представлен пример реализации диагностирования распределенной РСН, состоящей из местного диспетчерского пункта и 12 удаленных необслуживаемых терминалов, по состояниям “авария”, “ухудшение”, “норма”.*

Ключевые слова: *контроль технического состояния, надежность, диагностика, радиотехническая система, сеть связи, канал связи, радиопеленгация, топология, критерии работоспособности, отказ, печатный узел.*

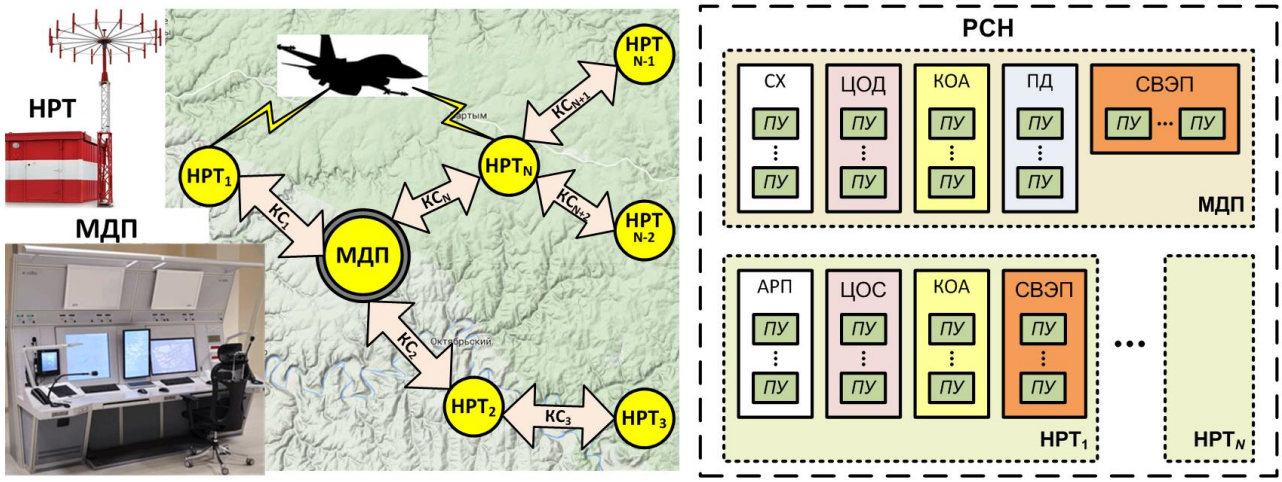
Актуальность

Несмотря на бурное развитие глобальных навигационных систем спутникового позиционирования, радиопеленгация широко применяется и в настоящее время, поскольку в удаленных и малоосвоенных районах не обнаруживаемые автоматические радиопеленгаторы (АРП) являются одним из основных средств обеспечения полетов [1].

Распределенная на местности радиотехническая система наблюдения (РСН) [2], имеющая топологию сети типа многоуровневая звезда, состоит из аппаратуры местного диспетчерского пункта (МДП), каналов связи и необслуживаемых радиотехнических терминалов (НРТ), которые могут быть удалены от МДП на расстояния до нескольких сотен километров (рис. 1 а). В обобщенном виде состав аппаратуры НРТ и МДП представлен на рис. 1 б.

В обобщенном виде аппаратура МДП состоит из следующих основных блоков: центра обработки данных (ЦОД), каналообразующей аппаратуры (КОА) для связи с НРТ, пульта диспетчера (ПД), системы хранения (СХ) пеленгационной и служебной информации, системы вторичного электропитания (СВЭП). Аппаратура НРТ имеет в своем составе

автоматический радиопеленгатор, блок цифровой обработки сигналов (ЦОС) и управления, КОА для связи с МДП, и СВЭП.



а) б)

Рис. 1. Распределенная на местности РСН (а) и состав ее аппаратуры (б)

Каждый основной блок может иметь в своем составе несколько печатных узлов (ПУ): ЦОД и ЦОС могут состоять из основной процессорной, резервной, интерфейсной и контроллерной плат; КОА может содержать ПУ маршрутизаторов, распределителей, преобразователей для разных типов линий связи; ПД включает ПУ индикации, ввода, отображения, дисплеи; СВЭП может иметь основные и резервные ПУ для различных напряжений питания; СХ может иметь основные и резервные твердотельные и НЖМД накопители, буферные ПУ; АРП может иметь ПУ для управления антенной, фильтрации и АЦП.

Постановка задачи

Поскольку важность работоспособности РСН высока, а удаленные терминалы являются необслуживаемыми, актуальной является задача обеспечения ее надежной работы. Для обеспечения надежной работы [3], в том числе, необходимо периодическое и систематическое диагностирование составных частей и модулей РСН, которые могут иметь несколько технических состояний (ТС).

Проблемам диагностирования распределенных радиотехнических систем и радиоэлектронной аппаратуры посвящены работы отечественных ученых Пархоменко П. П., Ведешенкова В. А., Увайсова С. У., зарубежных Брюле Д. Д., Рассела Й. Д., Кайма Ц. Р. и др. [4]. Несмотря на большой вклад этих ученых, проблемы диагностирования технических систем не достаточно разработаны. В частности, не рассмотрены вопросы диагностирования сложных пространственно-распределенных радиотехнических систем, имеющих много ТС на различных уровнях своей иерархии (от топологии сети до отдельных электронных компонентов). Поэтому актуальной является задача разработки новых концепций диагностирования РСН по *n*-мерному критерию.

Диагностирование распределенной РСН по бинарному критерию может быть для различных уровней глубины контроля γ:

- по топологии ($\gamma = 1$), учитываются ТС МДП ($ТС^{МДП}$) и всех НРТ ($ТС^{НРТ_N}$);
- до основного блока ($\gamma = 2$), учитываются ТС блоков ($ТС^{Блок}$);
- до печатного узла ($\gamma = 3$), учитываются ТС всех ПУ ($ТС^{ПУ_N^{Блок}}$);
- до электронного компонента ($\gamma = 4$).

Такое диагностирование с глубиной до $\gamma = 3$ можно описать выражениями:

для $\gamma = 1$:

$$ТС^{РСН} = ТС^{МДП} \& ТС^{НРТ_1} \& ... \& ТС^{НРТ_N};$$

для $\gamma = 2$:

$$\begin{cases} ТС^{МДП} = ТС^{КОА} \& ТС^{ЦОД} \& ТС^{СВЭП} \& ТС^{СХ} \& ТС^{ПД} \\ ТС^{НРТ} = ТС^{КОА} \& ТС^{ЦОС} \& ТС^{СВЭП} \& ТС^{АРП} \end{cases};$$

для $\gamma = 3$:

$$\begin{cases} ТС^{КОА} = ТС^{ПУ_1^{КОА}} \& ... \& ТС^{ПУ_N^{КОА}} \\ ТС^{АРП} = ТС^{ПУ_1^{АРП}} \& ... \& ТС^{ПУ_N^{АРП}} \\ ТС^{СВЭП} = ТС^{ПУ_1^{СВЭП}} \& ... \& ТС^{ПУ_N^{СВЭП}} \\ ТС^{ПД} = ТС^{ПУ_1^{ПД}} \& ... \& ТС^{ПУ_N^{ПД}} \\ ТС^{СХ} = ТС^{ПУ_1^{СХ}} \& ... \& ТС^{ПУ_N^{СХ}} \\ ТС^{ЦОД} = ТС^{ПУ_1^{ЦОД}} \& ... \& ТС^{ПУ_N^{ЦОД}} \\ ТС^{ЦОС} = ТС^{ПУ_1^{ЦОС}} \& ... \& ТС^{ПУ_N^{ЦОС}} \end{cases}. \quad (1)$$

При диагностировании распределенной РСН по множеству технических состояний РСН имеет $n^{РСН}$ ТС работоспособности, тогда в соответствие с ее топологией $n^{МДП}$ и $n^{НРТ}$ – число ТС МДП и НРТ, а в соответствие со структурой аппаратуры $n^{КОА}$, $n^{ЦОС}$, $n^{ЦОД}$, $n^{СВЭП}$, $n^{АРП}$, $n^{СХ}$, $n^{ПД}$ – число ТС ее основных блоков (в общем виде $n^{Блок}$). Поскольку в предлагаемых подходах предусмотрена глубина контроля γ до съемного ПУ, а полнота η до 100%, то каждый ПУ в общем случае также может иметь множество $n^{ПУ_i}$ ТС.

Подходы к диагностированию по множеству ТС

Очевидно, что интегральный критерий оценки работоспособности РСН будет зависеть от ТС ее ПУ. Можно применить три обоснованных подхода к определению ее ТС: методом наихудшего случая, методом усредненных диапазонов, методом с заданием приоритетов.

Рассмотрим суть метода наихудшего случая, в котором ТС РСН определяется как минимальное (min) из нормированных друг к другу значений ТС составных элементов РСН. Причем поскольку число ТС целое, используется функция $\|\bullet\|$ округления итогового ТС до ближайшего целого. Математически определение диагноза можно представить следующими выражениями:

для $\gamma = 1$:

$$TC^{РСН} = \left\| n^{РСН} \times \min\left(\frac{TC^{МДП}}{n^{МДП}}, \frac{TC^{НРТ_1}}{n^{НРТ}}, ..., \frac{TC^{НРТ_N}}{n^{НРТ}} \right) \right\|;$$

для $\gamma = 2$:

$$\begin{cases} TC^{МДП} = \left\| n^{МДП} \times \min\left(\frac{TC^{КОА}}{n^{КОА}}, \frac{TC^{ЦОД}}{n^{ЦОД}}, \frac{TC^{СВЭП}}{n^{СВЭП}}, \frac{TC^{СХ}}{n^{СХ}}, \frac{TC^{ПД}}{n^{ПД}} \right) \right\|; \\ TC^{НРТ} = \left\| n^{НРТ} \times \min\left(\frac{TC^{КОА}}{n^{КОА}}, \frac{TC^{ЦОС}}{n^{ЦОС}}, \frac{TC^{СВЭП}}{n^{НРТ}}, \frac{TC^{АРП}}{n^{АРП}} \right) \right\| \end{cases}$$

для $\gamma = 3$:

$$\begin{cases} TC^{КОА} = \left\| n^{КОА} \times \min\left(\frac{TC^{ПУ_1^{КОА}}}{n^{ПУ_1^{КОА}}}, ..., \frac{TC^{ПУ_N^{КОА}}}{n^{ПУ_N^{КОА}}} \right) \right\| \\ TC^{АРП} = \left\| n^{АРП} \times \min\left(\frac{TC^{ПУ_1^{АРП}}}{n^{ПУ_1^{АРП}}}, ..., \frac{TC^{ПУ_N^{АРП}}}{n^{ПУ_N^{АРП}}} \right) \right\| \\ TC^{СВЭП} = \left\| n^{СВЭП} \times \min\left(\frac{TC^{ПУ_1^{СВЭП}}}{n^{ПУ_1^{СВЭП}}}, ..., \frac{TC^{ПУ_N^{СВЭП}}}{n^{ПУ_N^{СВЭП}}} \right) \right\| \\ TC^{ПД} = \left\| n^{ПД} \times \min\left(\frac{TC^{ПУ_1^{ПД}}}{n^{ПУ_1^{ПД}}}, ..., \frac{TC^{ПУ_N^{ПД}}}{n^{ПУ_N^{ПД}}} \right) \right\| \\ TC^{СХ} = \left\| n^{СХ} \times \min\left(\frac{TC^{ПУ_1^{СХ}}}{n^{ПУ_1^{СХ}}}, ..., \frac{TC^{ПУ_N^{СХ}}}{n^{ПУ_N^{СХ}}} \right) \right\| \\ TC^{ЦОД} = \left\| n^{ЦОД} \times \min\left(\frac{TC^{ПУ_1^{ЦОД}}}{n^{ПУ_1^{ЦОД}}}, ..., \frac{TC^{ПУ_N^{ЦОД}}}{n^{ПУ_N^{ЦОД}}} \right) \right\| \\ TC^{ЦОС} = \left\| n^{ЦОС} \times \min\left(\frac{TC^{ПУ_1^{ЦОС}}}{n^{ПУ_1^{ЦОС}}}, ..., \frac{TC^{ПУ_N^{ЦОС}}}{n^{ПУ_N^{ЦОС}}} \right) \right\| \end{cases} \quad (2)$$

Суть метода усредненных диапазонов заключается в следующем: итоговый критерий вычисляется как среднее арифметическое нормированных критериев работоспособности составных частей. Математически это выражается следующим образом:

для $\gamma = 1$:

$$TC^{РСН} = \left\| \frac{n^{РСН}}{N+1} \times \left(\frac{TC^{МДП}}{n^{МДП}} + \sum_{i=1}^{N} \frac{TC^{НРТ_i}}{n^{НРТ_i}} \right) \right\|$$

для $\gamma = 2$:

$$\begin{cases} TC^{МДП} = \left\| \frac{n^{МДП}}{5} \times \left(\frac{TC^{КОА}}{n^{КОА}} + \frac{TC^{ЦОД}}{n^{ЦОД}} + \frac{TC^{СВЭП}}{n^{СВЭП}} + \frac{TC^{СХ}}{n^{СХ}} + \frac{TC^{ПД}}{n^{ПД}} \right) \right\| \\ TC^{НРТ} = \left\| \frac{n^{НРТ}}{4} \times \left(\frac{TC^{КОА}}{n^{КОА}} + \frac{TC^{ЦОС}}{n^{ЦОС}} + \frac{TC^{СВЭП}}{n^{НРТ}} + \frac{TC^{АРП}}{n^{АРП}} \right) \right\| \end{cases}$$

для $\gamma = 3$:

$$TC^{Блок} = \left\| \frac{n^{Блок}}{N} \times \sum_{i=1}^{N} \frac{TC^{ПУ_i^{Блок}}}{n^{ПУ_i^{Блок}}} \right\|, \quad (3)$$

где $N+1$ – число всех НРТ и МДП, а $\|\bullet\|$ – округление до ближайшего целого, так как число ТС – целое, $TC^{Блок}$ – техническое состояние основного блока (КОА, ЦОД, ЦОС, СВЭП и др.).

Суть метода с заданием приоритетов заключается в задании весовых коэффициентов k для МДП и каждого НРТ, всех блоков и ПУ аппаратуры, причем для каждого уровня глубины $\sum k_i = 1$. Такую приоритезацию можно задать выражениями:

для $\gamma = 1$:

$$TC^{РСН} = f\left(k^{МДП} \times \frac{n^{РСН} \times TC^{МДП}}{n^{МДП}}, k^{НРТ_1} \frac{n^{РСН} \times TC^{НРТ_1}}{n^{НРТ}}, ..., k^{НРТ_N} \frac{n^{РСН} \times TC^{НРТ_N}}{n^{НРТ}} \right)$$

для $\gamma = 2$:

$$\begin{cases} TC^{МДП} = f\left(\begin{array}{l} k^{КОА} \times \frac{n^{МДП} \times TC^{КОА}}{n^{КОА}}, k^{ЦОД} \times \frac{n^{МДП} \times TC^{ЦОД}}{n^{ЦОД}}, k^{СВЭП} \times \frac{n^{МДП} \times TC^{СВЭП}}{n^{СВЭП}}, \\ k^{СХ} \times \frac{n^{РСН} \times TC^{СХ}}{n^{СХ}}, k^{ПД} \times \frac{n^{РСН} \times TC^{ПД}}{n^{ПД}} \end{array} \right) \\ TC^{НРТ} = f\left(k^{КОА} \times \frac{n^{НРТ} \times TC^{КОА}}{n^{КОА}}, k^{ЦОС} \times \frac{n^{НРТ} \times TC^{ЦОС}}{n^{ЦОС}}, k^{СВЭП} \times \frac{n^{НРТ} \times TC^{СВЭП}}{n^{НРТ}}, k^{АРП} \times \frac{n^{НРТ} \times TC^{АРП}}{n^{АРП}} \right) \end{cases}$$

для $\gamma = 3$:

$$TC^{Блок} = f\left(k^{ПУ_1^{Блок}} \times \frac{n^{Блок} \times TC^{ПУ_1^{Блок}}}{n^{ПУ_1^{Блок}}}, ..., k^{ПУ_N^{Блок}} \times \frac{n^{Блок} \times TC^{ПУ_N^{Блок}}}{n^{ПУ_N^{Блок}}} \right) \quad (4)$$

где f – это функция, по которой определяется итоговое ТС, например min или усреднение диапазонов.

Комбинированный критерий оценки заключается в использовании любого из вышеизложенных методов (минимального, среднеарифметического и с заданием приоритетов) на различных уровнях иерархии РСН. Например,

топология может рассчитываться по среднеарифметическому, ПУ по минимальному, а блоки по приоритетам.

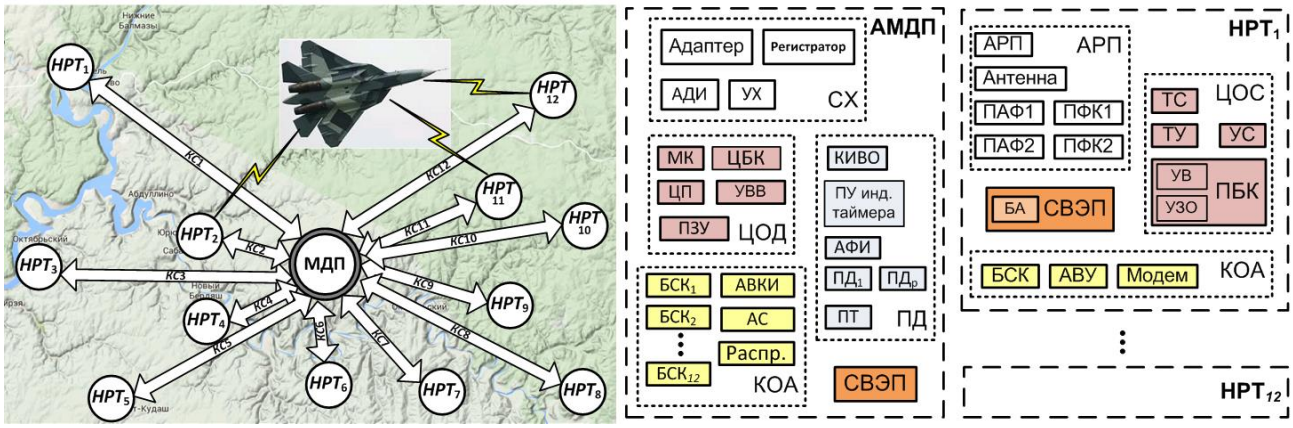
Для всех предложенных методов на различных уровнях глубины γ значения полноты η контроля определяются следующим образом:

$$\eta^{РСН} = \begin{cases} N_Д^T / (N+1), \gamma = 1 \\ N_Д^Б / N^Б, \gamma = 2 \\ N_Д^{ПУ} / N^{ПУ}, \gamma = 3 \end{cases}, \quad (5)$$

где $N_Д^T$, $N_Д^Б$, $N_Д^{ПУ}$ – число диагностируемых элементов топологии, всех диагностируемых блоков и всех диагностируемых ПУ распределенной РСН соответственно, $N+1$ – число МДП и НРТ, $N^Б$ и $N^{ПУ}$ – число всех блоков и ПУ в РСН. Иными словами полнота контроля показывает степень достоверности итогового ТС, полученного в результате диагноза.

Пример диагностирования РСН с тремя ТС

В практической реализации [5] распределенная РСН и все ее элементы до ПУ имеют три ТС (ухудшение, авария, норма) $n^{РСН} = n^{МДП} = n^{НРТ} = n^{КОА} = n^{ЦОС} = n^{ЦОД} = n^{СВЭП} = n^{АРП} = n^{СХ} = n^{ПД}$, $\eta = 100\%$, $\gamma = 3$. Интегральный критерий ТС определяется методом наихудшего случая. Топология и состав аппаратуры такой РСН представлены на рис. 2.



а) б)

Рис. 2. Топология (а) и состав аппаратуры (б) РСН

РСН состоит из МДП и 12 НРТ. В состав аппаратуры МДП входят следующие ПУ: микроконтроллер (МК), плата центрального процессора (ЦП), устройство ввода-вывода (УВВ); центральный блок контроля (ЦБК), ПЗУ; 12 блоков сопряжения с каналом (БСК), аппаратура ввода картографической информации (АВКИ), аппаратура сопряжения (АС), распределитель (Распр.); контрольный индикатор воздушной обстановки (КИВО), индикатор таймера, аппаратура формирования изображения, основной и резервный пульты диспетчера ($ПД_1$ и $ПД_Р$), пульт техника (ПТ); СВЭП; аппаратура документирования информации (АДИ), устройство хранения (УХ); плата адаптера, регистратор.

В состав аппаратуры НРТ входят: периферийный блок контроля (ПБК) с устройствами ввода (УВ) и защиты от ошибок (УЗО), устройство согласования (УС), ПУ телеуправления (ТУ) и телесигнализации (ТС); блок сопряжения с каналом (БСК), аппаратура вторичного уплотнения (АВУ), модем; СВЭП с блоком автоматики (БА); ПУ АРП, антенна, преобразователи аналог-фаза (ПАФ), фаза-код (ПФК).

В соответствие с составом, имеется следующее распределение ПУ по блокам: для МДП – 5 в ЦОД, 15 в КОА; 1 в СВЭП, 6 в ПД, 4 в СХ; для НРТ – 6 в ЦОС, 3 в КОА; 2 в СВЭП, 6 в АРП. Итоговые критерии определения ТС такой РСН определяются выражениями:

для $\gamma = 1$:

$$TC^{РСН} = \min\left(TC^{МДП}, TC^{НРТ_1}, ..., TC^{НРТ_{12}}\right);$$

для $\gamma = 2$:

$$\begin{cases} TC^{МДП} = \min\left(TC^{КОА}, TC^{ЦОД}, TC^{СВЭП}, TC^{СХ}, TC^{ПД}\right) \\ TC^{НРТ} = \min\left(TC^{КОА}, TC^{ЦОС}, TC^{СВЭП}, TC^{АРП}\right) \end{cases};$$

для $\gamma = 3$:

$$\begin{cases} TC^{КОА\_МДП} = \min\left(TC^{ПУ_1^{КОА}}, ..., TC^{ПУ_{15}^{КОА}}\right) \\ TC^{КОА\_НРТ} = \min\left(TC^{ПУ_1^{КОА}}, ..., TC^{ПУ_3^{КОА}}\right) \\ TC^{АРП} = \min\left(TC^{ПУ_1^{АРП}}, ..., TC^{ПУ_6^{АРП}}\right) \\ TC^{СВЭП\_МДП} = TC^{ПУ^{СВЭП}} \\ TC^{СВЭП\_НРТ} = \min\left(TC^{ПУ_1^{СВЭП}}, TC^{ПУ_2^{СВЭП}}\right) \\ TC^{ПД} = \min\left(TC^{ПУ_1^{ПД}}, ..., TC^{ПУ_6^{ПД}}\right) \\ TC^{СХ} = \min\left(TC^{ПУ_1^{СХ}}, ..., TC^{ПУ_4^{СХ}}\right) \\ TC^{ЦОД} = \min\left(TC^{ПУ_1^{ЦОД}}, ..., TC^{ПУ_5^{ЦОД}}\right) \\ TC^{ЦОС} = \min\left(TC^{ПУ_1^{ЦОС}}, ..., TC^{ПУ_6^{ЦОС}}\right) \end{cases} \quad (6)$$

Во всех случаях ТС может принимать одно из 3-х значений: 0 – авария, 1 – ухудшение, 2 – норма. Полнота контроля 100% означает диагностирование всех ПУ системы. Таким образом, при заданных значениях получается довольно простой в реализации механизм определения критериев работоспособности.

Выводы

Основанные на известных математических функциях определения минимума, усреднения, методе весовых коэффициентов и их комбинаций, впервые предложенные подходы к диагностированию технического состояния

распределенной РСН по множеству технических состояний предоставляют возможность разработчику наиболее гибко сформировать конфигурацию системы технического диагностирования, а именно: задавать любое число технических состояний для каждого элемента на всех уровнях иерархии; задавать глубину и рассчитывать полноту контроля.

На основе метода наихудшего случая из предложенного теоретического базиса можно, например, реализовать вычислительно несложную автоматизированную систему технического диагностирования 12-ти терминальной распределенной РСН по 3-м техническим состояниям, с глубиной контроля до съемного ПУ и полнотой 100%.

Исследование выполнено при финансовой поддержке Российского Научного Фонда (проект № 16-49-02021).

Литература

1. Аминев Д. А., Журков А. П., Козырев А. А., Увайсов С. У. Алгоритмы работы программного обеспечения микропроцессорных систем контроля аппаратуры пеленгаторной позиции // Труды НИИР. 2014. № 3. С. 11–17.

2. Аминев Д. А., Журков А. П., Козырев А. А. Алгоритм контроля аппаратуры местного диспетчерского пункта наземной локальной радиопеленгационной системы наблюдения // Труды НИИР. 2015. № 4. С. 72–78.

3. Журков А. П., Аминев Д. А., Кулыгин В. Н. Модель надежности распределенной радиотехнической системы наблюдения минимальной конфигурации // В кн.: Труды Международного симпозиума «НАДЕЖНОСТЬ И КАЧЕСТВО»: в 2 т. Т. 1. Пенза: ПГУ, 2016. С. 120–122.

4. Журков А. П., Аминев Д. А., Гусева П. А., Мирошниченко С. С., Петросян П. А. Анализ возможностей применения подходов самодиагностирования к распределенной радиотехнической системе наблюдения // Системы управления, связи и безопасности. 2015. № 4. С. 114–122. URL: http://sccs.intelgr.com/archive/2015-04/06-Zhurkov.pdf (дата обращения 02.10.2016).

5. Журков А. П. Протокол организации обмена контрольно-диагностической информацией распределенной радиотехнической системы наблюдения // Качество. Инновации. Образование. 2016. № 4. С. 61–71.

References

1. Aminev D. A., Zhurkov A. P., Kozyrev A. A., Uvaysov S. U. Algoritmy raboty programmnogo obespechenija mikroprocessornyh sistem kontrolja apparatury pelengatornoj pozicii [The algorithms used in the software of microprocessor systems for monitoring equipment direction finding position]. *Trudy NIIR*, 2014, no. 3, pp. 11-17 (in Russian).

2. Aminev D. A., Zhurkov A. P., Kozyrev A. A., Algoritm kontrolja apparatury mestnogo dispetcherskogo punkta nazemnoj lokal'noj radiopelengacionnoj sistemy

nabljudenija [The control algorithm for local control point equipment of RDF system]. *Trudy NIIR*, 2015, no. 4, pp. 72-78 (in Russian).

3. Zhurkov A. P., Aminev D. A., Kulygin V. N. Model' nadezhnosti raspredelennoj radiotehnicheskoj sistemy nabljudenija minimal'noj konfiguracii [Reliable model for minimum configuration of distributed radio direction finding system]. *Trudy Mezhdunarodnogo simpoziuma «NADEZHNOST" I KACHESTVO»*, 2016, no. 1, pp. 120-122 (in Russian).

4. Zhurkov A. P., Aminev D. A., Guseva P. A., Miroshnichenko S. S., Petrosjan P. A. Analysis of the Possibilities of Self-Diagnosis Approaches to Distributed Electronic Surveillance System. *Systems of Control, Communication and Security*, 2015, no. 4, pp. 114-122. Available at: http://sccs.intelgr.com/archive/2015-04/06-Zhurkov.pdf (accessed 2 October 2016) (in Russian).

5. Zhurkov A. P. Protokol organizacii obmena kontrol'no-diagnosticheskoj informaciej raspredelennoj radiotekhnicheskoj sistemy nablyudeniya [Protocol of the organization of exchange for control and diagnostic information of distributed radio direction finding system]. *Kachestvo. Innovacii. Obrazovanie*, 2016, no. 4, pp. 61-71 (in Russian).

Статья поступила 29 сентября 2016 г.

Информация об авторах

Аминев Дмитрий Андреевич – кандидат технических наук, старший научный сотрудник. Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова Российской академии наук. Область научных интересов: системы и сети передачи данных; радиоэлектронная аппаратура. E-mail: aminev.d.a@ya.ru.

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

Журков Александр Петрович – аспирант Департамента электронной инженерии. Московский институт электроники и математики Национального исследовательского университета Высшая школа экономики. Область научных интересов: диагностирование радиотехнических систем; системы управления связью. E–mail: petrovyc@gmail.com.

Адрес: 123458, Россия, г. Москва, Таллинская ул., д. 34.

Кроткова Карина Георгиевна – студент 4-го курса кафедры ИУ-4 "Проектирование и технология производства электронной аппаратуры". Московский государственный технический университет им. Н.Э. Баумана. Область научных интересов: моделирование радиотехнических систем; сбор и обработка информации. E–mail: ilanit184@gmail.com.

Адрес: 105005, Россия, г. Москва, 2-я Бауманская ул., д. 5, стр. 1.

Охломенко Илья Вячеславович – магистрант 1-го курса кафедры ИУ-4 "Проектирование и технология производства электронной аппаратуры". Московский государственный технический университет им. Н.Э. Баумана. Область научных интересов: моделирование радиотехнических систем; проектирование цифровой аппаратуры. E–mail: ilya.okhlomenko@gmail.com.

Адрес: 105005, Россия, г. Москва, 2-я Бауманская ул., д. 5, стр. 1.

Research offers for Diagnosing of Distributed Radio Direction Finding Systems with a Some Set of Technical States

D. A. Aminev, A. P. Zhurkov, K. G. Krotkova, I. V. Ohlomenko

Formulation of the problem. *Modern radio direction finding systems (RDFS) are used in remote and underdeveloped areas for control of flight operations. To ensure the reliability requirements of RDFS necessary make it diagnose. Existing diagnostic methods allow determining the technical condition (TC) as a binary criterion, which is not suitable for distributed RDFS having a plurality of TC because its have the spatial distributed and the complex hierarchy and the multi-module structure. Therefore,* ***the aim of the paper*** *is develop means of diagnosis of distributed RDFS with different types of TC to various levels of its hierarchy. For this in paper offers the mathematical methods for describe of the determining integral TC criteria.* ***Result.*** *New means based on known mathematical principles are offered for the diagnosis of distributed RDFS which has the some set of technical conditions. For means of diagnosis of RDFS is used: the worst-case method, the method of average range, the priority method. The paper has an example as RDFS is diagnose if it consist of the local dispatch center and 12 the remote unattended terminals which have different TC.*

Keywords: *technical condition monitoring, reliability, diagnostics, radio system, the communication network, the communication channel, radio direction finding, topology, performance criteria, rejection, printed circuit board.*

Information about Authors

Dmitrij Andreevich Aminev – Ph.D. of Engineering Sciences, Senior Researcher. V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. E–mail: aminev.d.a@ya.ru.

Address: 117997, Moscow, 65 Profsoyuznaya str.

Aleksandr Petrovich Zhurkov – The postgraduate student of the Department of Electronic Engineering. Moscow Institute of Electronics and Mathematics National Research University Higher School of Economics. Field of research: diagnostics of technical systems; communication control system. E–mail: petrovyc@gmail.com.

Address: Russia, 123458, Moscow, ul. Tallinskaya, 34.

Karina Georgievna Krotkova – Student of the Department of "Design and technology of electronic equipment". Bauman Moscow State Technical University. Field of research: modeling of radio systems; digital hardware design. E–mail: ilanit184@gmail.com.

Ilya Vyacheslavovich Ohlomenko – Student of the Department of "Design and technology of electronic equipment". Bauman Moscow State Technical University. Field of research: modeling of radio systems; digital hardware design. E-mail: ilya.okhlomenko@gmail.com.

Address: Russia, 105005, Moscow, ul. Baumanskaya 2-ya, 5.

УДК 004.7: 623.618

Информационное оружие в технической сфере: терминология, классификация, примеры

Макаренко С. И.

Актуальность. *Адекватное описание противоборства в информационной сфере требует формирования соответствующего терминологического базиса. Одним из основных элементов этого базиса является понятие «информационное оружие». При этом теория информационного оружия в психологической сфере, а также его применение для влияния на социально-политические процессы достаточно глубоко разработана в имеющихся работах. Однако терминологический аппарат в области понятий и классификации информационного оружия в технической сфере отличается противоречивостью и неоднозначностью. В связи с этим уточнение терминологии в области информационно-технического оружия и проведение его системной классификации является актуальной задачей.* ***Целью работы*** *является уточнение терминологического базиса в области информационного оружия в технической сфере, а также введение его строгой классификации.* ***Новизной работы*** *является авторский подход к системе терминов, определений и классификации информационно-технического оружия и информационно-технический воздействий, основанный на методах системного анализа и логического обобщения известных работ. Также к элементам новизны стоит отнести выявленные частные тенденции развития наиболее распространенных средств информационно-технического воздействия.* ***Практическая значимость.*** *Представленный анализ может быть использован техническими специалистами для обоснования новых технологических решений в области информационной безопасности, а также военными специалистами – для обоснования новых форм и способов информационного противоборства. Кроме того, данный анализ будет полезен научным работникам и соискателям, ведущим научные и диссертационные исследования для прикладного обоснования целесообразности предлагаемых ими улучшений безопасности информационных систем.*

Ключевые слова: *информационное противоборство, информационное оружие, информационно-техническое оружие, информационно-техническое воздействие, удаленные сетевые атаки, сетевые атаки, вирусы, программные закладки, аппаратные закладки, нейтрализаторы тестовых программ, ложные объекты информационного пространства, средства моделирования боевых действий, средства технической разведки, средства разведки по отрытым источникам, Большие Данные.*

Введение

Адекватное описание противоборства в информационной сфере потребовало формирования соответствующего терминологического базиса. В США и странах НАТО еще с 90-х годов введены руководящие документы, определяющие терминологию и, зачастую, именно ей руководствуются исследователи в области информационного противоборства. Обзор этой терминологии представлен в более ранней работе автора [1]. Вместе с тем за пределами анализа, выполненного в этой работе, осталось понятие информационного оружия. При этом теория информационного оружия в психологической сфере и его применение для влияния на социально-политические процессы достаточно широко представлена в работах таких специалистов как: И.Н. Панарин, Г.Г. Почепцов, А.В. Манойло, С.П. Расторгуев, С.Г. Кара-Мурза, В.В. Цыганов, С.Н. Бухарин, Д.А. Новиков, А.Г. Чхартишвили, а также других ученых. Однако терминологический аппарат

в области понятий и классификации информационного оружия в технической сфере отличается противоречивостью и неоднозначностью. В качестве примера можно привести работы С.Н. Гриняева [2], А.В. Бедрицкого [3], В.К. Новикова [4], С.А. Петренко [5], Л.В. Воронцовой, Д.Б. Фролова [6], Н.П. Шеховцеова, Ю.Е. Кулешова [7], Е.Д. Паршаковой [8]. Представленные в этих работах варианты классификации информационного оружия в технической сфере и информационно-технических воздействий не обладают высокой степенью систематизации, и зачастую ведутся без учета методов системного подхода. К наиболее систематизированному изложению понятий информационного оружия можно отнести словарь [9]. Однако, представленные в этом словаре понятия не объединены к строгую классификационную систему.

В связи с вышеуказанным, в статье предлагается авторский подход к системе терминов, определений и классификации информационно-технического оружия и информационно-технический воздействий. В основу статьи положены материалы открытых источников, а именно – анализ руководящих документов Вооруженных сил (ВС) США в области информационного противоборства [1], дополненный материалом публикаций отечественных специалистов в данной предметной области.

Структурно статья состоит из трех разделов:

1) информационное оружие – анализ терминологии, а также его классификация;
2) информационно-техническое оружие – анализ терминологии; определения информационно-технического оружия и информационно-технических воздействий, а также их классификация;
3) наиболее распространенные средства информационно-технического воздействия – анализ способов и примеров применения, определений и квалификация для наиболее распространенных средств:
    - удаленных сетевых атак;
    - вирусов;
    - программных закладок;
    - аппаратных закладок;
    - нейтрализаторов тестовых программ;
    - ложных объектов информационного пространства;
    - средств моделирования боевых и военных действий;
    - средств технической разведки;
    - средств компьютерной разведки;
    - средств разведки по открытым источникам.

1. Информационное оружие

1.1 Определение информационного оружия

В настоящее время нередко к информационному оружию относят широкий класс приемов и способов информационного воздействия на противника – от дезинформации и пропаганды до средств радиоэлектронной борьбы. При этом на сегодняшний день нет единого толкования понятия

«информационное оружие». В различных источниках приводятся различные определения этого понятия. При этом наиболее общим является следующее.

Информационное оружие – совокупность средств информационного воздействия на технику и людей [2, 10].

В соответствии со сферами, в которых ведется информационное противоборство, информационное оружие подразделяется на два основных вида [2, 10]:

1) информационно-техническое оружие;
2) информационно-психологическое (также включает в себя психофизическое оружие).

Главными объектами информационного оружия первого вида является техника, второго – люди.

Психофизическое оружие – это совокупность всех возможных методов и средств (технотронных, суггестивных, психотропных, комплексных и др.) скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении. Психофизическое оружие представляет собой разновидность информационно-психологического оружия [2, 11].

Фактически информационное оружие является технологией, включающей в себя [2, 12]:

- анализ способов и механизмов активизации у конкретной информационной системы противника, свойственных ей программ самоуничтожения, деградации или дестабилизации;
- поиск такой программы;
- разработка конкретного информационного оружия;
- применение информационного оружия по заданному объекту.

Полковник ВВС США Р. Сафрански, один из идеологов концепции сетецентрической войны, дает достаточно широкое определение информационному оружию.

Информационное оружие – использование специально подобранных средств, под воздействием которых происходит изменение процессов в информационных и в социальных системах в соответствии с поставленными целями [13]. В соответствии с разработанной Р. Сафрански концепцией, применять информационное оружие предполагается на стратегическом, оперативном и тактическом уровнях. При этом основными объектами его воздействия являются информационно-технические системы, социальные системы, отдельные личности или группы лиц (то есть групповое и индивидуальное сознание) [13].

Оригинальный подход к определению понятия «информационное оружие» сделан в работе [14]. В соответствии с этой работой дано следующее определение.

Информационное оружие – различные средства поражения: высокоточное оружие для поражения органов управления или отдельных радиоэлектронных средств, средства радиоэлектронной борьбы, источники

мощного электромагнитного импульса, программные вирусы и др., эффективно решающие задачи информационной войны [14].

Спорным в данном подходе является отнесение к классу информационного оружия большинства средств поражения и физического оружия по той лишь причине, что оно обеспечивает физическое уничтожение органов управления и радиоэлектронных систем (РЭС) противника.

В работах [15] и [16] приводятся близкие по смыслу определения информационного оружия.

Информационное оружие – совокупность информационных технологий, способов и средств информационного воздействия, предназначенных для ведения информационной войны [15].

Информационное оружие – оружие, наиболее эффективно решающее задачи информационной войны, основной задачей которой является достижение информационного превосходства [16].

Указывая на недостаток двух приведенных выше определений информационного оружия, заключающийся в привязке данного понятия к неоднозначно трактуемому в различных источниках понятию «информационная война», автор монографии [11] приводит следующее определение этого вида оружия.

Информационное оружие – это средства информационного воздействия на технику и людей с целью решения задач воздействующей стороны, и специфичные способы их применения [11].

Это определение, а также определение, представленное в работах [2, 10], на взгляд автора являются наиболее общими и полными и включают в себя всю совокупность средств для организации воздействий, которые могут быть использованы для деструктивного влияния как в технической, так и в психологической сфере.

В работе [13] авторами сделана другая попытка обобщения и конкретизации вышеуказанных определений информационного оружия.

Информационное оружие – это совокупность способов и средств [13]:

- подавления элементов инфраструктуры государственного и военного управления противника;
- электромагнитного влияния на элементы информационных и телекоммуникационных систем;
- несанкционированного доступа к информационным ресурсам с последующей их деформацией, уничтожением или хищением;
- информационно-психологического воздействия на военнослужащих и гражданское население противоборствующей стороны.

Информационному оружию присущи следующие качественные характеристики, которыми оно отличается от других видов оружия [17]:

- универсальность – его применение не зависит от климатических и географических условий, времени суток, сезонов года и т.п.;
- скрытость – для его применения не требуется проводить мобилизацию, создавать большие группировки войск, в то же время его действие

незаметно, а по воздействию сопоставимо с оружием массового поражения;
- внезапность применения – не требуется его длительная подготовка;
- экономическая эффективность – разработка информационного оружия и его применение требует существенно меньших затрат по сравнению с другими видами оружия;
- масштабность применения как для решения задач стратегического, так и тактического уровня;
- эффект «цепной реакции» – воздействие информационного оружия на отдельный элемент информационной системы информационного ресурса может привести к выводу из строя других элементов системы, а затем и системы в целом;
- сложность осуществления контроля за созданием и испытанием информационного оружия – его разработку, а в ряде случаев и сам факт применения можно надежно скрыть от разведки противника.

При этом темпы совершенствования информационного оружия (как, впрочем, и любого вида атакующего вооружения) превышают темпы развития технологий защиты и противодействия ему [2].

1.2 Общая классификация информационного оружия

В соответствии со сферой своего применения информационное оружие подразделяется на [13]:
- информационно-техническое оружие;
- информационно-психологическое оружие.

В соответствии со своим целевым назначением информационное оружие подразделяется на два типа [13]:
- оборонительное информационное оружие;
- наступательное информационное оружие.

Оборонительное информационное оружие решает задачи обороны в информационной войне и включает системы многоуровневой информационной безопасности и различные системы противодействия информационно-психологическому оружию противника. Таким образом, в состав оборонительной составляющей информационного оружия входят средства противодействия и нейтрализации наступательного информационного оружия противника [13].

Наступательное информационное оружие решает задачи воздействия на систему принятия решения противника путем поражения наиболее критичных ее компонентов (как в технической, так и психологической сферах) [13].

2. Информационно-техническое оружие

2.1 Определение и классификация информационно-технического оружия

Особенностью информационно-технического оружия является его ориентированность на поражение аппаратно-программных средств систем передачи, хранения и обработки информации, функционирующих в технической сфере информационного пространства (в киберпространстве).

Взяв за основу определения информационного оружия, ориентированного на применение в технической сфере, представленные в работах [2, 7, 18], можно дать следующее определение.

Информационно-техническое оружие – совокупность специально организованной информации, информационных технологий, способов и средств, позволяющих целенаправленно изменять (уничтожать, искажать), копировать, блокировать информацию, преодолевать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, нарушать функционирование систем обработки информации, дезорганизовывать работу технических средств, компьютерных систем и информационно-вычислительных сетей, а также другой инфраструктуры высокотехнологического обеспечения жизни общества и функционирования системы управления государством, применяемое в ходе информационной операции для достижения поставленных целей.

В соответствии с этим определением информационно-техническое оружие включает технические и программные средства, обеспечивающие несанкционированный доступ к базам данных, нарушение штатного режима функционирования аппаратно-программных средств, а также вывод из строя ключевых элементов информационной инфраструктуры отдельного государства или группы государств.

В соответствии с различными основаниями, информационно-техническое оружие можно классифицировать следующим образом (рис. 1).

1. По цели использования информационно-техническое оружие делят на [2]:
   - обеспечивающее;
   - атакующее;
   - комбинированное.

Рассматривая данную классификацию, надо отметить, что традиционно, средства оборонительных информационно-технических воздействий не рассматриваются в качестве оборонительного информационно-технического оружия. В настоящее время сложился подход, в котором оборонительные средства (средства антивирусной защиты, системы обнаружения и предотвращения вторжений, средства криптографической защиты и т.д.) рассматриваются как элемент обеспечения информационной безопасности и противодействия несанкционированному доступу со стороны некоторых отдельных нарушителей. Вместе с тем в условиях, когда будет вестись информационное противоборство в технической сфере, такой подход может

вызвать путаницу в определениях, и потребует введения категории «оборонительное информационно-техническое оружие».

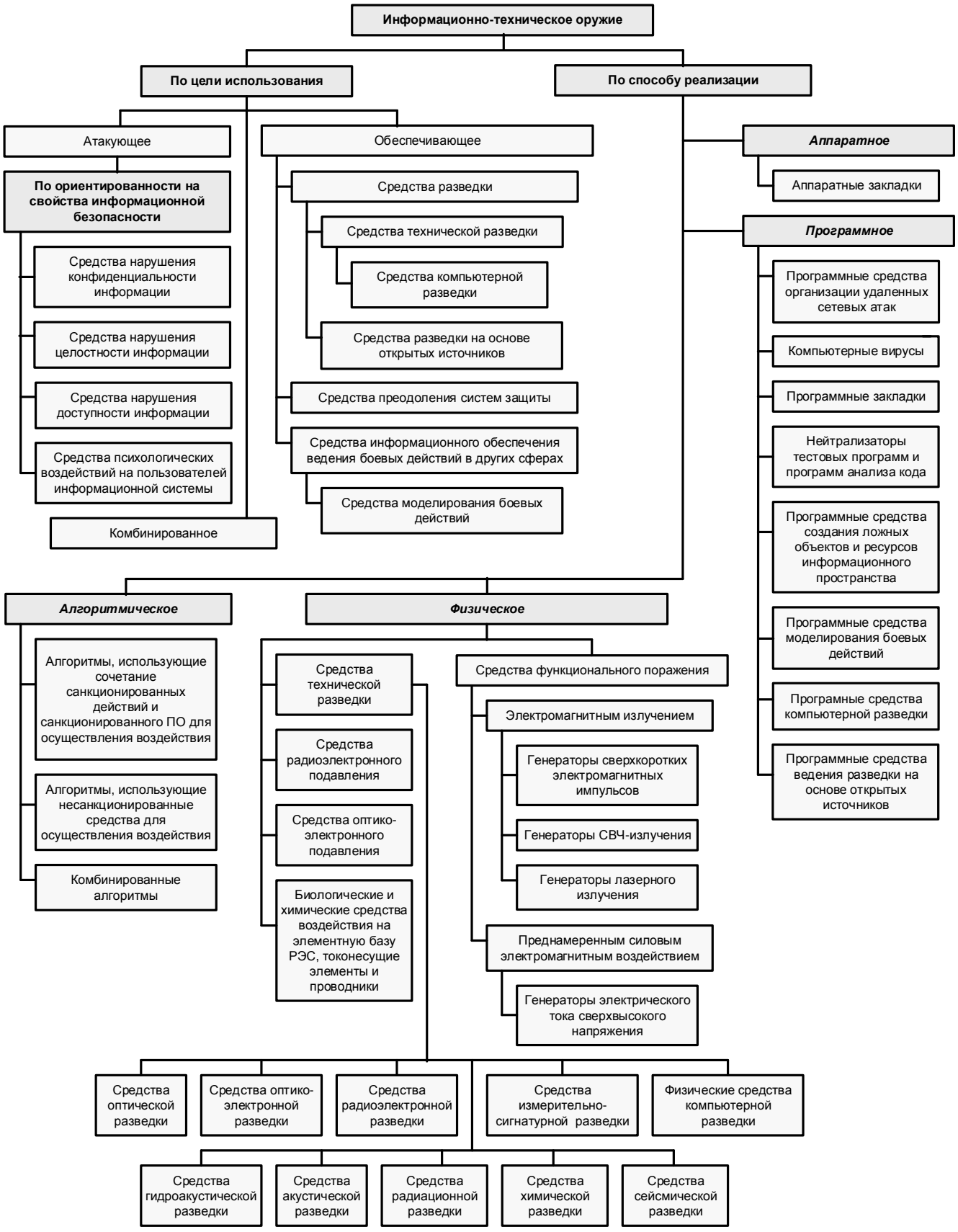


Рис. 1. Классификация информационно-технического оружия

Обеспечивающее информационно-техническое оружие применяется для сбора данных, обеспечивающих эффективное применение оборонительного или атакующего информационно-технического и другого оружия, а также против средств защиты атакуемой системы [2].

Обеспечивающее информационно-техническое оружие можно разделить на:

1) средства разведки:
   - традиционные средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
   - средства компьютерной разведки (как программные, так и доступа к физической инфраструктуре);
   - средства ведения разведки на основе открытых источников;
2) средства преодоления систем защиты;
3) средства информационного обеспечения ведения боевых действий в других сферах.

Необходимо отметить, что средства разведки почти всегда выступают в качестве обеспечивающего оружия. Они позволяют получить информацию об атакующих средствах информационно-технического оружия противника и способах его применения, что позволяет более рационально сконфигурировать собственные средства информационно-технической защиты. Воздействие средств разведки проявляется как в виде пассивных действий, направленных на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

Успешное применение средств преодоления систем защиты позволяет осуществлять эффективные воздействия на хранимую, обрабатываемую и передаваемую в системе информацию с использованием атакующего информационно-технического оружия.

Отдельно стоит выделить средства информационного обеспечения ведения боевых действий в других сферах. Под такими средствами понимаются не автоматизированные системы управления и различного рода комплексы автоматизации, а комплексы для моделирования боевых действий, которые позволяют путем многократного прогона модели найти рациональный состав сил и средств, а также оптимальную стратегию их действий при любом вероятном сценарии действий противника.

Атакующее информационно-техническое оружие – оружие, с помощью которого осуществляется воздействие на хранимую, обрабатываемую и передаваемую в системе информацию, нарушающее используемые в системе информационные технологии [2].

Атакующее информационно-техническое оружие, в зависимости от его ориентированности на нарушение конкретного свойства информационной безопасности, можно разделить на четыре основных вида [2]:

- средства нарушения конфиденциальности информации;
- средства нарушения целостности информации;

- средства нарушения доступности информации;
- средства психологических воздействий на пользователей информационной системы.

Применение атакующего информационно-технического оружия направлено на срыв выполнения информационной системой целевых задач.

Как правило, атакующее информационно-техническое оружие включает в себя следующие компоненты, объеденные в единую систему [19]:

- средство доставки оружия;
- средство преодоления подсистемы защиты атакуемой системы;
- полезная нагрузка.

2. По способу реализации информационно-техническое оружие можно разделить на следующие классы [2, 7]:

- алгоритмическое;
- программное;
- аппаратное;
- физическое.

Информационно-техническое оружие, относящееся к разным классам, может применяться совместно. Кроме того, некоторые виды информационно-технического оружия могут одновременно нести в себе черты нескольких классов.

К **алгоритмическому информационно-техническому оружию** относятся [2]:

- алгоритмы, использующие сочетание санкционированных действий и санкционированного (легального) программного обеспечения для осуществления несанкционированного воздействия на информационные ресурсы;
- алгоритмы использования несанкционированных средств (другого информационно-технического оружия – программного, аппаратного, физического) для осуществления несанкционированного воздействия на информационные ресурсы;
- комбинированные алгоритмы, состоящие из алгоритмов предыдущих двух типов.

Разновидностью алгоритмического оружия являются *эксплойт* (exploit) – потенциально невредоносный набор данных (например, санкционированная последовательность команд, графический файл или сетевой пакет нестандартного размера, запрос на установление соединения), который некорректно обрабатывается информационной системой, работающей с такими данными, вследствие ошибок в ней. Результатом некорректной обработки такого набора данных может быть перевод информационной системы в уязвимое состояние.

Примером алгоритмического оружия является DoS-атака (Denial of Service – отказ в обслуживании) заключающаяся в том, что на атакуемую систему с высокой интенсивностью посылаются корректные запросы на использование ее информационных ресурсов. Это ведет к тому, что возможности информационной системы по обслуживанию таких запросов

быстро исчерпываются, и она отказывает в обслуживании всем своим пользователям.

К **программному информационно-техническому оружию** относятся программное обеспечение, которое может быть использовано для проведения атак на информационные системы противника, и позволяющее в процессе своей работы производить несанкционированное воздействие на ее информационные ресурсы. К такому программному обеспечению можно отнести:

- программные средства организации удаленных сетевых атак;
- компьютерные вирусы;
- программные закладки;
- нейтрализаторы тестовых программ и программ анализа кода.

Кроме того, к программному информационно-техническому оружию можно отнести ряд программных средств, решающих обеспечивающие задачи, как в информационном пространстве, так и в традиционных сферах применения оружия (воздух, земля, море):

- программные средства создания ложных объектов и ресурсов информационного пространства (виртуальные машины);
- программные средства моделирования боевых действий;
- программные средства компьютерной разведки;
- программные средства ведения разведки по открытым источникам в семантической части информационного пространства.

К **аппаратному информационному оружию** могут быть отнесены аппаратные средства, которые изначально встроены в информационную систему или несанкционированно внедренные в нее, а также санкционированные аппаратные средства, обладающие недекларируемыми возможностями, которые позволяют в процессе своей работы производить несанкционированное воздействие на информационные ресурсы системы. К наиболее распространенному типу аппаратного информационно-технического оружия относятся аппаратные закладки.

К **физическому информационно-техническому оружию** могут быть отнесены средства добывания информации путем доступа к физической инфраструктуре информационного пространства, анализу генерируемых этой инфраструктурой физических полей, а также средства радиоэлектронного и огневого поражения ее физических элементов. При этом, некоторые специалисты считают более корректным отнесение к физическому информационно-техническому оружию только средств, предназначенных исключительно для воздействия на технические элементы информационной системы.

Обобщение сведений, представленных в работах [7, 13] показал, что классификация физического информационно-технического оружия может иметь вид:

- средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
- средства радиоэлектронного подавления (РЭП);

- средства оптико-электронного подавления;
- средства функционального поражения электромагнитным излучением (ЭМИ) – генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения и др.;
- средства функционального поражения преднамеренными силовыми электромагнитными воздействиями – генераторы электрического тока сверхвысокого напряжения;
- биологические и химические средства воздействия на элементную базу радиоэлектронных систем (РЭС), их токонесущие элементы и проводники (например, графитовые бомбы).

2.2 Определение и классификация информационно-технических воздействий

Информационно-техническое воздействие (ИТВ) – основной поражающий фактор информационно-технического оружия, представляющий собой воздействие либо на информационный ресурс, либо на информационную систему или на средства получения, передачи, обработки, хранения и воспроизведения информации в ее составе, с целью вызвать заданные структурные и/или функциональные изменения.

Объекты информационно-технического воздействия – информация, ее свойства, связанные с информационной безопасностью, информационно-технические системы (системы связи и управления, телекоммуникационные системы, радиоэлектронные средства, компьютерные сети и т.д.), технические средства, компьютерные системы и информационно-вычислительные сети, а также другая инфраструктура высокотехнологического обеспечения жизни общества и функционирования системы управления государством.

Различают следующие **виды информационно-технических воздействий**:

- одиночные;
- групповые.

Информационно-технические воздействия также классифицируют по характеру поражающих свойств [2, 10]:

- высокоточные воздействия (например, на определенный ресурс в информационно-вычислительной сети);
- комплексные воздействия (например, вся информационно-телекоммуникационная инфраструктура).

По типу воздействий на информацию или информационный ресурс информационно-технические воздействия могут быть:

- пассивными:
  - перехват;
  - несанкционированный доступ;
- активными:
  - разрушающие воздействия;
  - манипулирующие воздействия;

- блокирующие воздействия;
- отвлекающие.

Пассивные воздействия не оказывают непосредственного влияния на работу информационной системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование информационной системы приводит к тому, что пассивное воздействие трудно обнаружить. Примером пассивного воздействия является разведка параметров информационной системы.

Активные воздействия оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Очевидной особенностью активного воздействия, в отличие от пассивного, является принципиальная возможность его обнаружения, так как в результате его осуществления в информационной системе происходят определенные деструктивные изменения.

По цели использования информационно-технические воздействия могут быть классифицированы на:

- обеспечивающие;
- атакующие;
- оборонительные;
- комбинированные.

По способу реализации информационно-технические воздействия могут быть разделены на:

- алгоритмические;
- программные;
- аппаратные;
- физические:
  - электромагнитные (среди них отдельно можно выделить воздействия на основе различных электромагнитных волн: радиоэлектронные; оптико-электронные; оптические; электрические)
  - акустические;
  - гидроакустические;
  - радиационные;
  - химические;
  - биологические;
  - на основе новых и других физических принципов.

Классификация информационно-технических воздействий в общем случае по смыслу совпадает с классификацией информационно-технического оружия, за исключением оборонительных воздействий. Традиционно, средства оборонительных информационно-технических воздействий не рассматриваются в качестве оборонительного информационно-технического оружия, вместе с тем они существуют и играют одну из ведущих ролей в информационном противоборстве при организации защиты собственной стороны.

Оборонительные информационно-технические воздействия ориентированы на противодействие информационно-техническому оружию противника. Их можно классифицировать следующим образом:

- *выявляющие* – воздействия, ориентированные на выявление как самого факта, так и последовательности атакующих воздействий противника;
- *блокирующие* – воздействия, ориентированные на блокировку атакующих воздействий противника;
- *контр-атакующие* – воздействия на информацию, информационные ресурсы и информационную инфраструктуру противника с целью срыва его атакующих воздействий;
- *отвлекающие* – воздействия, ориентированные на дезинформацию противника, отвлечение его атакующих или обеспечивающих воздействий на незначащие или ложные объекты;
- *противодействие обеспечивающим воздействиям противника* – способы маскировки, обеспечения безопасности, повышения скрытности реальных режимов функционирования, а также мониторинга каналов утечки в отношении собственных информационных систем.

Схема классификации информационно-технических воздействий представлена на рис. 2.

Средства информационно-технического воздействия – средства, используемые в качестве информационно-технического оружия или для защиты от него [2].

Необходимо отметить, что классификация атакующих и обеспечивающих информационно-технических воздействий в общем виде совпадает с классификацией соответствующих видов информационно-технического оружия. Однако необходимость защиты от атакующих и обеспечивающих информационно-технических воздействий противника позволяет дополнительно выделить так называемые оборонительные средства информационно-технического воздействия, к которым можно отнести:

- средства антивирусной защиты;
- системы обнаружения и предотвращения вторжений;
- средства криптографической защиты;
- стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
- средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;
- средства тестирования программного обеспечения и анализа кода для выявления программных закладок и недекларируемых возможностей;
- средства создания ложных объектов и ресурсов в информационном пространстве.

Применительно к новейшим разработкам атакующего информационно-технического оружия наибольшее развитие получили средства специального программно-математического воздействия, которые объединяют возможности алгоритмического и программного информационно-технического оружия.

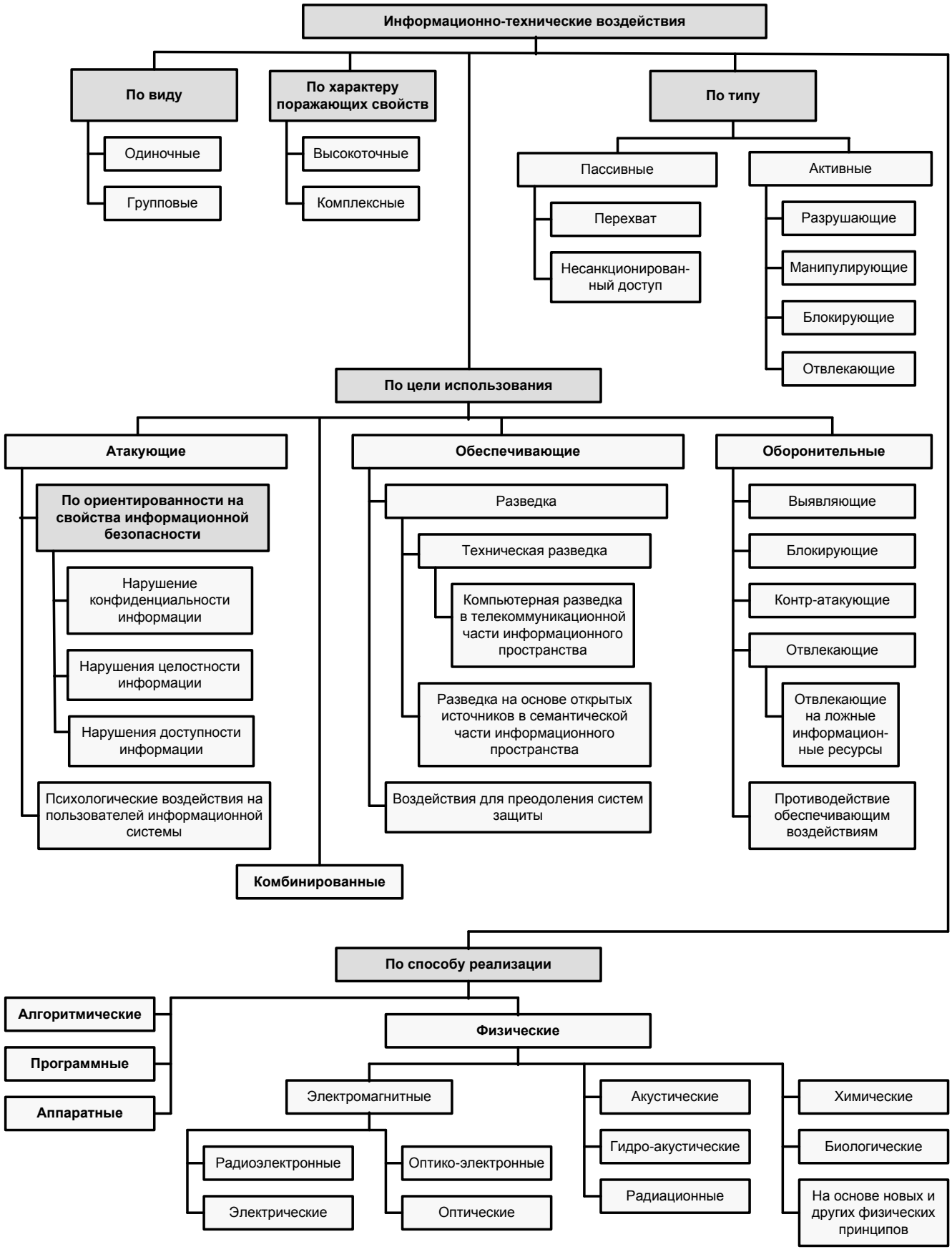


Рис. 2. Классификация информационно-технических воздействий

Средства специального программно-математического воздействия – некоторая программа или комплекс программ, способные выполнить любое подмножество перечисленных ниже функций [2, 20]:

- скрывать признаки своего присутствия в программно-аппаратной среде информационной системы;
- обладать способностью к самокопированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать) код программ в памяти информационной системы;
- сохранять фрагменты информации из памяти информационной системы в некоторой области внешней памяти прямого доступа (локальной и удаленной);
- искажать, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных;
- подавлять информационный обмен в телекоммуникационных сетях, фальсифицировать информацию, передаваемую по каналам управления;
- противодействовать работе тестовых программ и систем защиты информационных ресурсов.

При этом под самокопированием понимается процесс воспроизведения своего собственного кода (в том числе и в модифицированном виде) в оперативной или внешней памяти системы с последующим его внедрением. Под ассоциированием с другой программой понимается интеграция своего кода, либо его части в код другой программы таким образом, чтобы при некоторых условиях управление передавалось на код программы с потенциально опасными последствиями [2].

К основным средствам информационно-технического воздействия, классифицированным по способу реализации, можно отнести:

1) алгоритмические (атакующие):
   - эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйверы, BIOS);
   - эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
   - эксплойты, ориентированные на сетевые протоколы информационной системы;
   - эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования (например, вирус Stuxnet, внедренный в АСУ технологическим процессом обогащения урана, за счет перехвата и модификации команд от

промышленного контролера, в течение длительного времени задавал для центрифуг нештатный режим работы, что привело к отказу более 1000 центрифуг на Иранском заводе по обогащению урана);

2) программные:
   - атакующие:
     - компьютерные вирусы;
     - программные закладки;
     - нейтрализаторы тестовых программ и программ анализа кода;
   - обеспечивающие:
     - программные средства для моделирования боевых действий;
     - программные средства компьютерной разведки в телекоммуникационной части информационного пространства;
     - программные средства ведения разведки на основе открытых источников в семантической части информационного пространства;
   - оборонительные:
     - программные средства антивирусной защиты;
     - системы обнаружения и предотвращения вторжений;
     - программные средства криптографической защиты;
     - программные стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
     - средства тестирования программного обеспечения и анализа кода для выявления программных закладок и недекларируемых возможностей;
     - средства создания ложных объектов и ресурсов в информационном пространстве.
3) аппаратные:
   - атакующие:
     - аппаратные закладки;
   - оборонительные:
     - средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;
4) физические:
   - атакующие:
     - средства РЭП;
     - средства оптико-электронного подавления;
     - средства функционального поражения электромагнитным излучением (генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения);
     - средства и комплексы функционального поражения преднамеренными силовыми электромагнитными

воздействиями (генераторы электрического тока сверхвысокого напряжения);

- биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники (например, графитовые бомбы).

- обеспечивающие:
  - средства технической разведки (в том числе и средства компьютерной разведки).

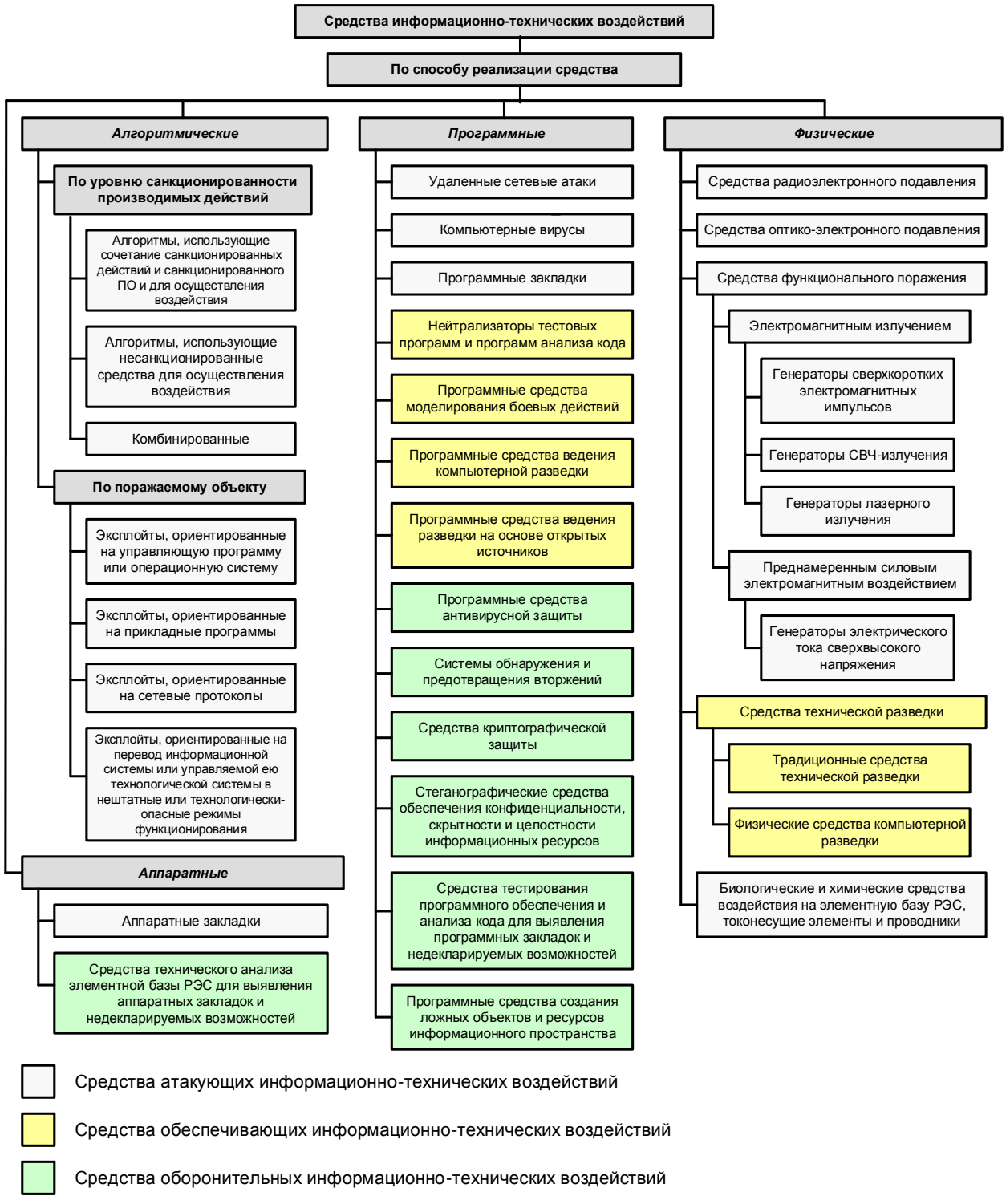


Рис 3. Классификация средств информационно-технического воздействия

Отдельно необходимо отметить следующее. К средствам технической разведки, представленным в данной классификации, относятся те средства, которые добывают информацию об атакующих средствах информационно-технического оружия противника и способах его применения, т.е. являются средствами обеспечивающего информационного оружия. Средства технической разведки могут оказывать воздействие на объекты противника как путем пассивных действий, направленные на добывание информации, что, как правило, связанно с нарушением ее конфиденциальности, так и путем активных действий (атак), направленных на создание условий, благоприятствующих добыванию информации.

Схема классификации средств информационно-технических воздействий представлена на рис. 3.

Рассмотрим более подробно наиболее распространенные средства информационно-технического воздействия из представленных на рис. 3. Виду того, что антивирусные средства защиты, системы обнаружения и предотвращения вторжений, а также криптографические и стеганографические средства защиты довольно подробно рассмотрены в известной литературе (например, в работе [21]), то основное внимание уделим следующим информационно-техническим воздействиям и средствам их проведения:

- удаленные сетевые атаки;
- компьютерные вирусы;
- программные закладки;
- аппаратные закладки;
- нейтрализаторы тестовых программ и программ анализа кода;
- средства создания ложных объектов информационного пространства;
- средства моделирования боевых действий;
- средства технической разведки (средства компьютерной разведки рассмотрены отдельно);
- средства разведки по отрытым источникам в глобальном информационном пространстве.

3. Наиболее распространенные средства информационно-технического воздействия

3.1 Удаленные сетевые атаки

3.1.1 Определение и классификация удаленных сетевых атак

С учетом определения и классификации удаленных воздействий на распределенные вычислительные системы, представленные в работе [22], можно дать следующее определение.

Удаленная сетевая атака – это разрушающее или дестабилизирующее информационно-техническое воздействие, осуществляемое по каналам связи удаленным относительно атакуемой системы субъектом и характерное для структурно- и пространственно-распределенных информационных систем.

Удаленные сетевые атаки становятся возможными благодаря уязвимостям в существующих протоколах обмена данными и в подсистемах защиты распределенных информационных систем. При этом к основным уязвимостям информационных систем, которые позволяют проводить против них успешные удаленные сетевые атаки, относятся [21, 22]:

- открытость информационной системы, свободный доступ к информации по организации сетевого взаимодействия, способам защиты применяемых в системе;
- наличие ошибок в операционных системах, прикладном программном обеспечении, протоколах сетевого обмена;
- разнородность используемых версий программного обеспечения и операционных систем;
- сложность организации защиты межсетевого взаимодействия;
- ошибки конфигурирования систем и средств защиты;
- неправильное или ошибочное администрирование систем;
- несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации эксплойтов и ошибок в программном обеспечении;
- «экономия» на средствах и системах обеспечения безопасности или игнорирование их.

В соответствии с различными основаниями удаленные сетевые атаки можно классифицировать следующим образом (рис. 4).

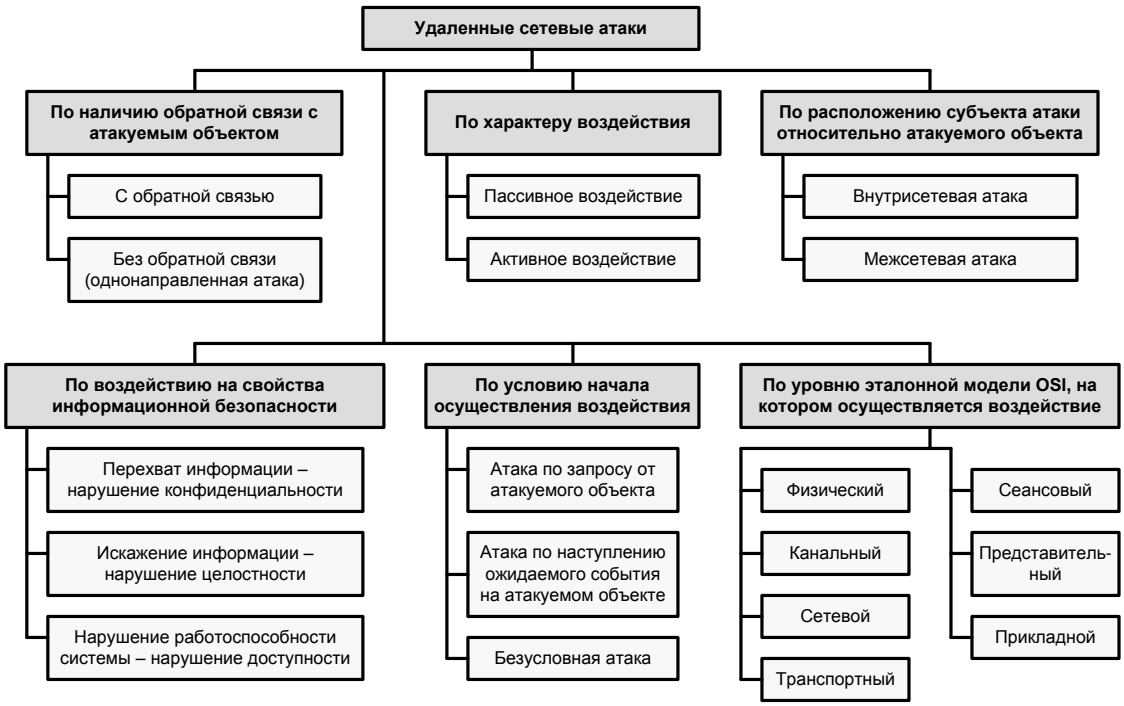


Рис. 4. Классификация удаленных сетевых атак

1. По характеру воздействия [21, 22]:

- пассивное воздействие;
- активное воздействие.

Пассивное воздействие не оказывает непосредственного влияния на работу информационной системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование атакуемой системы приводит к тому, что пассивную сетевую атаку практически невозможно обнаружить. Примером типовой пассивной удаленной сетевой атаки является прослушивание канала связи.

Активное воздействие оказывает непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Практически все типы удаленных сетевых атак относятся к активным воздействиям. Очевидной особенностью активного воздействия, по сравнению с пассивным, является принципиальная возможность его обнаружения, так как в результате его осуществления в информационной системе происходят определенные деструктивные изменения.

2. По воздействию на свойства информационной безопасности [21, 22]:

- перехват информации – нарушение конфиденциальности информационных ресурсов системы;
- искажение информации – нарушение целостности информационных ресурсов системы;
- нарушение работоспособности системы – нарушение доступности информационных ресурсов.

Перехват информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. В этом случае осуществляется несанкционированный доступ к информации без возможности ее искажения. Также очевидно, что нарушение конфиденциальности информации является пассивной сетевой атакой. Примером такой атаки, связанной с перехватом информации может служить прослушивание канала в сети.

Искажение информации означает либо полный контроль над информационным потоком между объектами распределенной системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, искажение информации ведет к нарушению целостности информационных ресурсов системы. Примером удаленной сетевой атаки, целью которой является нарушение целостности информационных ресурсов, может служить атака, связанная с внедрением ложного сетевого объекта в систему, например внедрения ложного DNS-сервера.

При нарушении работоспособности системы атакующей стороной не предполагается получение несанкционированного доступа к информации. Ее основная цель – добиться, чтобы элементы распределенной информационной системы на атакуемом объекте вышли из строя, а для всех остальных объектов системы доступ к информационным ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить DoS-атака.

3. По условию начала осуществления воздействия [21, 22]:

- атака по запросу от атакуемого объекта;

- атака по наступлению ожидаемого события на атакуемом объекте;
- безусловная атака.

При атаке по запросу от атакуемого объекта атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов могут служить DNS- и ARP-запросы. Важно отметить, что данный тип удаленных атак наиболее характерен для распределенных сетевых информационных систем.

При атаке по условию наступления ожидаемого события, атакующий осуществляет наблюдение за состоянием информационной системы, которая является целью атаки. При возникновении определенного события в этой системе атакующий начинает воздействие на нее. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сама атакуемая система. Такие сетевые атаки довольно распространенны. Примером такой атаки может быть атака, связанная с несанкционированным доступом к информационным ресурсам компьютера по сети после факта его успешного заражения backdoor-вирусом, который создает дополнительные уязвимости в подсистеме защиты компьютера.

При безусловной атаке она осуществляется немедленно и безотносительно к состоянию информационной системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

4. По наличию обратной связи с атакуемым объектом [21, 22]:

- с обратной связью;
- без обратной связи (однонаправленная атака).

Удаленная сетевая атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ. Следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адаптивно реагировать на все изменения, происходящие на атакуемом объекте. Подобные удаленные атаки наиболее характерны для распределенных сетевых информационных систем.

В отличие от атак с обратной связью, удаленным сетевым атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную сетевую атаку можно называть однонаправленной удаленной атакой. Примером такой однонаправленной атаки может служить DoS-атака.

5. По расположению субъекта атаки относительно атакуемого объекта [21, 22]:

- внутрисетевая атака;
- межсетевая атака.

В случае внутрисетевой атаки, субъект и объект атаки находятся в одной сети. При межсетевой атаке субъект и объект атаки находятся в разных сетях.

Важно отметить, что межсетевая удаленная атака представляет гораздо большую опасность, чем внутрисетевая. Это связано с тем, что в случае межсетевой атаки ее объект и непосредственно атакующий могут находиться на значительном расстоянии друг от друга, что может существенно воспрепятствовать мерам по отражению атаки.

6. По уровню эталонной модели OSI, на котором осуществляется воздействие [21, 22]:

- физический;
- канальный;
- сетевой;
- транспортный;
- сеансовый;
- представительный;
- прикладной.

Удаленные атаки могут быть ориентированны на сетевые протоколы, функционирующие на различных уровнях модели OSI. При этом надо отметить, что атаки, ориентированные на физический, канальный, сетевой и транспортный уровни, как правило, направлены против сетевой инфраструктуры – оборудования узлов сети и каналы связи. Атаки, ориентированные на сеансовый, представительный и прикладной уровни, как правило, направлены против оконечных терминалов сети. В связи с этим, в зависимости от уровня OSI, на который ориентирована атака, конкретный вид используемого воздействия может значительно меняться. Это может быть воздействие средств РЭП или ЭМИ при атаке, ориентированной на физический уровень, при этом эффекты от такого воздействия отображаются на более верхних уровнях модели OSI. Либо DoS-атака на узловое оборудование сети, либо вирус поражающий операционную систему конечного терминального оборудования.

3.1.2 Примеры способов информационно-технических воздействий на основе удаленных сетевых атак

В связи с тем, что удаленные сетевые атаки, совместно с воздействием вирусных средств, составляют подавляющее большинство всех информационно-технических воздействий, рассмотрим их более подробно.

К основным способам и средствам информационно-технического воздействия, которые можно классифицировать как удаленные сетевые атаки, относятся (рис. 5) [21, 22]:

- анализ сетевого трафика;
- подмена доверенного объекта или субъекта информационной системы;
- внедрение ложного объекта в информационную систему:
    - внедрение ложного объекта путем навязывания ложного сетевого маршрута;
    - внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети;

- путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
- путем формирования потока ложных ответов не дожидаясь запросов от узлов сети;

- использование ложного сетевого объекта для организации удаленной атаки на информационную систему:
  - селекция информации и сохранение ее на ложном сетевом объекте;
  - модификация информации, проходящей через ложный сетевой объект;
  - подмена информации, проходящей через ложный сетевой объект;
- атаки, типа «отказ в обслуживании»:
  - отказ в обслуживании (DoS-атака);
  - распределенная атака «отказ в обслуживании» (DDoS-атака);
  - зацикливание процедуры обработки запроса.

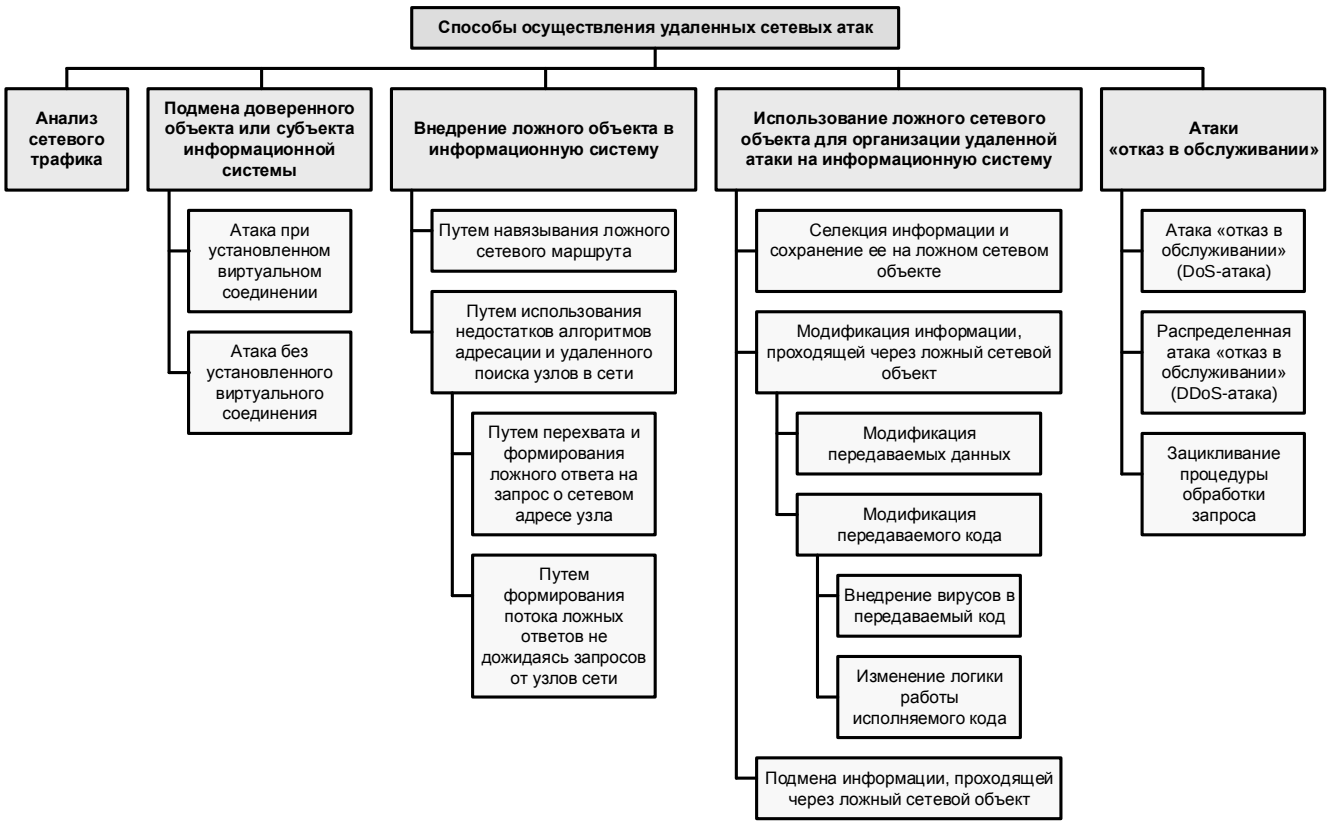


Рис. 5. Классификация способов осуществления удаленных сетевых атак

Анализ сетевого трафика. Основной особенностью сетевой информационной системы является то, что ее объекты распределены в пространстве и связь между ними осуществляется по сетевым соединениям. Таким образом, сообщения и данные, пересылаемые между объектами информационной системы, передаются по каналам связи в виде пакетов. Эта особенность привела к появлению специфичного для сетевой информационной

системы удаленного воздействия, заключающегося в прослушивании канала связи. Данное воздействие называется *анализом сетевого трафика*.

Анализ сетевого трафика позволяет [21, 22]:

- изучить логику работы сетевой информационной системы, то есть получить взаимно однозначное соответствие событий, происходящих в системе, команд и данных, пересылаемых друг другу ее объектами, в момент появления этих событий. Это достигается путем перехвата и анализа пакетов сетевого трафика. Знание логики работы информационной системы позволяет смоделировать и осуществлять другие удаленные сетевые атаки;
- перехватить поток данных, которыми обмениваются объекты сетевой информационной системы. Таким образом, эта атака заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером информации, перехваченной при помощи данной типовой удаленной атаки, могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети.

В соответствии с выше представленной классификацией анализ сетевого трафика является пассивным воздействием. Осуществление данной атаки без обратной связи ведет к нарушению конфиденциальности информации внутри одного сегмента сети на канальном или сетевом уровне OSI. При этом начало осуществления атаки безусловно по отношению к цели атаки [21, 22].

Подмена доверенного объекта или субъекта информационной системы. Одной из проблем безопасности сетевой информационной системы является недостаточная идентификация и аутентификация ее объектов удаленных друг от друга. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами сетевого взаимодействия. Обычно в сетевых информационных системах эта проблема решается следующим образом – в процессе создания виртуального канала объекты системы обмениваются определенной информацией, уникально идентифицирующей данный канал. Однако такой обмен производится не всегда. Зачастую, особенно при передаче служебной и адресной информации в сети, используются одиночные сообщения, не требующие подтверждения. Так как сетевой адрес достаточно просто подделывается, его можно использовать для виртуальной подмены доверенного объекта или субъекта информационной системы. Таким образом, в том случае, когда в сети используются нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной удаленная атака *подмена доверенного объекта или субъекта информационной системы*, заключающаяся в передаче по сети сообщений от имени произвольного объекта или субъекта информационной системы [21, 22].

Существуют две разновидности этой сетевой атаки, в зависимости от принятой в системе политики информационной безопасности и подхода к защите сетевых соединений [21, 22]:

- атака при установленном виртуальном соединении;
- атака без установленного виртуального соединения.

В случае если в сети для сеанса обмена данными устанавливаются виртуальные соединения, атака будет заключаться в присвоении прав доверенного субъекта сетевого взаимодействия, легально подключившегося к объекту системы. Это позволит атакующему вести сеанс работы с объектом информационной системы от имени доверенного субъекта. Реализация таких удаленных атак обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты системой как корректные). Однако, для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сетевых сообщений [21, 22].

Атаки на информационную систему, в которой не используются виртуальные соединения, заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов. В этом случае возможна подделка сетевого адреса отправителя. Например, так реализуется удаленная атака, использующая навязывание ложного маршрута, путем посылки ложных адресных сообщений [21, 22].

Подмена доверенного объекта или субъекта информационной системы может быть классифицирована как активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации по наступлению на атакуемом объекте определенного события. Такая удаленная атака может являться как внутрисетевой, так и межсетевой, как с обратной связью, так и без обратной связи с атакуемым объектом и осуществляться на сетевом или транспортном уровнях модели OSI [21, 22].

Внедрение ложного объекта в информационную систему. Зачастую в распределенной информационной системе бывают недостаточно надежно решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов), при их взаимодействии с объектами системы. В этом случае такая распределенная система может подвергнуться сетевой атаке, связанной с изменением параметров маршрутизации и внедрением в сеть ложного объекта. В том случае, если настройки сети таковы, что для взаимодействия объектов необходимо использовать алгоритмы удаленного поиска узлов, то это также может быть использовано для внедрения в систему ложного объекта.

Таким образом, существуют два принципиально разных способа проведения атаки «внедрение ложного объекта в информационную систему» [21, 22]:

- внедрение ложного объекта путем навязывания ложного сетевого маршрута;
- внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети:

- путем перехвата и формирования ложного ответа на запрос о сетевом адресе узла;
- путем формирования потока ложных ответов не дожидаясь запросов от узлов сети.

Современные глобальные сети представляют собой совокупность сетевых сегментов, связанных между собой через узлы-маршрутизаторы. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждой пары адресатов сети указывается оптимальный маршрут. Основная цель атаки, связанной с внедрением ложного объекта путем навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте сетевой информационной системы так, чтобы новый маршрут проходил через ложный объект сети – узел атакующего. Реализация этой атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. Данная атака проходит в две стадии [21, 22].

1. Атакующему необходимо от имени сетевых управляющих устройств (например, маршрутизаторов) произвести рассылку по сети специальных служебных сообщений, что приведет к изменению маршрутизации в сети. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, который будет проходить через его узел.
2. Атакующий наращивает количество трафика, перенаправленного через свой узел, и получает возможность вести прием, анализ и передачу сообщений, передаваемых по сети.

Внедрение ложного объекта путем навязывания ложного сетевого маршрута – активное воздействие, безусловное по отношению к цели атаки. Данная удаленная атака может осуществляться как внутри одного сегмента сети, так и межсетевым образом, как с обратной связью, так и без обратной связи с атакуемым объектом на сетевом, транспортном и прикладном уровне модели OSI [21, 22].

В распределенной информационной системе часто оказывается, что ее удаленные объекты изначально не имеют достаточно информации, необходимой для адресации передаваемых сообщений. Обычно такой информацией являются аппаратные и логические адреса объектов системы. Для получения подобной информации в распределенных системах используются различные алгоритмы удаленного поиска, заключающиеся в передаче по сети специальных поисковых запросов. После получения ответа на запрос, запросивший субъект системы обладает всеми необходимыми данными для адресации. Руководствуясь полученными из ответа сведениями об искомом объекте, запросивший субъект системы начинает передачу информации. Примером подобных запросов, на которых базируются алгоритмы удаленного поиска, могут служить ARP- и DNS-запросы в сети Internet [21, 22].

В случае использования в распределенной информационной системе механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать

данные, использование которых приведет к адресации на атакующий ложный узел. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через этот ложный объект информационной системы [21, 22].

Другой вариант внедрения в распределенную информационную систему ложного объекта использует недостатки алгоритма удаленного сетевого поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса, и тогда его ложный ответ будет немедленно принят и обработан. Такая удаленная атака чрезвычайно распространена в глобальных сетях, когда у атакующего, из-за нахождения его в другом сетевом сегменте относительно цели атаки, просто нет возможности перехватить поисковый запрос [21, 22].

Внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети – активное воздействие, совершаемое с целью нарушения конфиденциальности и целостности информации, которое может являться атакой по запросу от атакуемого объекта, а также безусловной атакой. Данная удаленная атака может быть как внутрисетевой, так и межсетевой, имеет обратную связь с атакуемым объектом и осуществляется на канальном, сетевом и прикладном уровнях модели OSI [21, 22].

Использование ложного объекта для организации удаленной атаки на систему. После внедрения ложного объекта в сеть и получением контроля над проходящим потоком информации в сети, ложный объект может применяться для различных способов воздействия на перехваченную информацию. Выделяют следующие основные воздействия на информацию, перехваченную ложным объектом [21, 22]:

- селекция информации и сохранение ее на ложном сетевом объекте;
- модификация информации, проходящей через ложный сетевой объект;
- подмена информации, проходящей через ложный сетевой объект.

Селекция информации и сохранение ее на ложном сетевом объекте является пассивной сетевой атакой, сходной с атакой «анализ сетевого трафика», которая дополнена динамическим семантическим анализом, производимом на ложном объекте. Вместе с тем наибольший интерес представляет возможность использования ложного объекта для модификации или подмены информации.

Рассматривают два основных вида модификации информации [21, 22]:

- модификация передаваемых данных;
- модификация передаваемого кода:
    - внедрение вирусов в передаваемый код;
    - изменение логики работы исполняемого кода.

Для модификации передаваемых данных на внедренном объекте производится селекция потока перехваченной информации и его анализ. При этом может быть распознан тип передаваемых файлов (исполняемый файл или файл, содержащий данные). При обнаружении файла данных появляется

возможность модифицировать эти данные, проходящие через ложный объект. При этом если модификация данных является достаточно стандартным воздействием, то на модификации передаваемого кода стоит остановиться отдельно.

Ложный объект, проводя семантический анализ информации, проходящей через него, может выделять среди потока информации файлы, содержащие исполняемый код. Для того, чтобы определить, что передается по сети – код или данные, необходимо распознавать определенные особенности, свойственные конкретным типам исполняемых файлов. При этом можно выделить два различных по цели вида модификации кода [21, 22]:

- внедрение вирусов в передаваемый код;
- изменение логики работы исполняемого кода.

При внедрении вирусов в передаваемый код к исполняемому файлу дописывается тело вируса, а также изменяется точка начала исполнения кода так, чтобы она указывала на начало кода внедренного вируса. Описанный способ, в принципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что файл оказывается заражен вирусом в момент передачи его по сети! Такое возможно лишь при использовании воздействия «внедрение ложного объекта» [21, 22].

При изменении логики работы исполняемого файла, при передаче его по сети происходит похожая модификация исполняемого кода. Однако ее цель – алгоритмическое воздействие, ориентированное на внедрение программных закладок, внесение в исполняемый файл дополнительных уязвимостей или эксполойтов. Сложностью такого воздействия является то, что для него, как правило, требуется предварительное исследование логики функционирования исполняемого файла [21, 22].

Внедрение ложного объекта позволяет не только модифицировать, но и подменять перехваченную им информацию. При возникновении в сети определенного контролируемого ложным объектом события, одному из участников обмена посылается заранее подготовленная дезинформация. При этом такая дезинформация, в зависимости от контролируемого события, может быть как исполняемым кодом, так и данными.

Отказ в обслуживании. В общем случае в сетевой информационной системе каждый ее субъект должен иметь возможность подключиться к любому объекту системы и получить в соответствии со своими правами удаленный доступ к его информационным ресурсам. Обычно в сетевых информационных системах возможность предоставления удаленного доступа реализуется следующим образом – на объекте системы запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. В случае получения запроса на соединение сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. Очевидно, что сервер способен отвечать лишь на ограниченное число запросов. Эти ограничения зависят от параметров информационной системы, пропускной способности ее сети и быстродействия ЭВМ, на которых он функционирует.

Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов за счет отправки большого числа запросов к нему.

Различают три типа этих удаленных атак.

1. *Отказ в обслуживании* (DoS-атака) – передача с одного адреса такого количества запросов на атакуемый объект, которое позволяет передать пропускная способность канала связи. В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) системы, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная блокировка объекта из-за невозможности системы заниматься ничем другим, кроме обработки запросов.
2. *Распределенная атака «отказ в обслуживании»* (DDoS-атака) – передача с нескольких объектов системы на другой атакуемый объект бесконечного числа запросов на подключение от имени этих или других объектов. Результатом применения этой удаленной атаки является нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов сетевой информационной системы.
3. *Зацикливание процедуры обработки запроса* – передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно переполнение буфера с последующим зависанием системы.

Удаленная сетевая атака «отказ в обслуживании» классифицируется как активное воздействие, осуществляемое с целью нарушения работоспособности системы, безусловная относительно цели атаки. Данная атака является однонаправленным воздействием, осуществляемым как межсетевым, так и внутрисетевым образом, осуществляемым на сетевом, транспортном и прикладном уровнях модели OSI [21, 22].

Наиболее распространенными способами осуществления атаки «отказ в обслуживании» являются следующие (рис. 6).

1. Способы, основанные на насыщении полосы пропускания системы – атаки, связанные с большим количеством, как правило, бессмысленных или сформированных в неправильном формате запросов к информационной системе или ее сетевому оборудованию, с целью обеспечить отказ в работе системы из-за исчерпания ее системных ресурсов (процессорного времени, памяти или пропускной способности каналов связи). К наиболее распространенным таким способам относятся [23]:

- атаки типа HTTP-flood и ping-flood;
- Smurf-атака (ICMP-flood);
- атака с помощью переполнения пакетами SYN в TCP соединении (SYN-flood).

Рис. 6. Наиболее распространенные способы осуществления атаки «отказ в обслуживании»

2. Способы, основанные на недостатке ресурсов системы – атаки, связанные с захватом или избыточным использованием ресурсов информационной системы. К наиболее распространенным таким способам относятся [23]:

- отправка «тяжелых» или «сложных» пакетов;
- переполнение сервера log-файлами;
- использование уязвимостей неправильно настроенной подсистемы управления ковтами использования системных ресурсов;
- использование уязвимостей недостаточной проверки данных пользователей;
- атаки, вызывающие ложные срабатывания подсистемы защиты информационной системы.

3. Способы, основанные на удаленном несанкционированном доступе за счет использования эксплойтов в программном обеспечении атакуемой системы. К наиболее распространенным таким способам относятся [23]:

- удаленное использование уязвимостей в программном коде операционной системы и прикладного программного обеспечения информационной системы;
- удаленное использование переполнения буфера программы;
- удаленное использование ошибок в разделении памяти между программами в защищенном режиме операционной системы.

4. Способы, основанные на использовании эксплойтов сетевых протоколов атакуемой системы. К наиболее распространенным таким способам относятся [23]:

- DoS-атаки, использующие уязвимости в программном обеспечении DNS-серверов;
- DDoS-атаки на DNS-серверы.

В настоящее время атаки типа «отказ в обслуживании» являются не только наиболее распространенными, но и наиболее опасными воздействиями. Так, в ноябре 2002 года была проведена глобальная DDoS-атака на корневые DNS-серверы с целью полного блокирования общедоступного сегмента сети Интернет. В результате этой атаки злоумышленники смогли вывести из строя 7 из 13 корневых DNS-серверов [23].

3.2 Компьютерные вирусы

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве боевых средств информационно-технического воздействия начато сравнительно недавно. При этом, несмотря на относительную молодость информационно-технических воздействий вирусного типа, уже зафиксировано несколько «волн» их применения для достижения стратегических целей. К первому случаю такого использования вируса относится применение в 2010 году вируса Stuxnet с целью срыва ядерной программы Ирана за счет инфицирования АСУ технологическим процессом обогащения урана. Как показывает анализ работ [24, 25, 26], к другим вирусам, которые также могут быть классифицированы как информационно-техническое оружие, можно также отнести: Flame, Duqu, Regin, Gauss, MiniFlame, MiniDuqu, Sputnik и др. Эксперты отмечают общие высокотехнологические черты данных вирусов, такие как: библиотеки (в том числе open source), среды, используемые уязвимости, приемы противодействия средствам защиты, а также высокое качество кода.

В отличие от своих «непрофессиональных собратьев» средства информационно-технического воздействия на основе вирусов обладают следующими особенностями функционирования [24]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей «нулевого» уровня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;
- гибкая система саморазмножения;
- инфраструктурная поддержка, обновление и управление;
- масштабируемость, наличие СУБД атак;
- высокое качество кода, и возможности обработки некорректных ситуаций.

Компьютерные вирусы в соответствии со способами распространения и вредоносной нагрузкой можно классифицировать по четырем основным типам [21]:

- классические вирусы;
- программы типа «червь»;
- программы типа «троян»;
- другие вредоносные программы.

Особенностью современных боевых вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам, и которые ориентированы на решение конкретной задачи (модули типа классический вирус – для саморазмножения в информационной системе, модули типа червь – для распространения по сети, модуль типа «троян» – для организации дестабилизирующего воздействия).

Кроме того, по способу хранения в памяти информационной системы компьютерные вирусы можно классифицировать на [27]:

- резидентные;
- нерезидентные.

Резидентные вирусы после активации хранят свои копии в оперативной памяти системы, способны перехватывать события операционной системы и программ (например, обращения к файлам или дискам) и инициировать при этом процедуры заражения обнаруженных объектов. Поэтому резидентные вирусы опасны не только во время работы инфицированной программы, но и после ее окончания. Резидентные копии таких вирусов остаются жизнеспособными вплоть до выключения или перезагрузки информационной системы [27].

Нерезидентные вирусы, напротив, активны на довольно непродолжительных интервалах времени – пока функционирует инфицированная вирусом программа [27].

Для защиты от обнаружения со стороны антивирусов и средств защиты информационной системы в вирусах могут применяться следующие технологии [21]:

- шифрование – вирус состоит из двух функциональных элементов: собственно, вирус и шифратор. При этом каждая конкретная копия вируса состоит из шифратора, собственного случайного ключа и собственно вируса, зашифрованного этим ключом;
- метаморфизм – создание различных копий вируса путем замены блоков команд на эквивалентные, путем перестановки местами участков кода, вставки между значащими участками кода незначаших команд и др.;
- перехват управления при обращении операционной системы или системы защиты к инфицированным элементам информационной системы.

Использование этих технологий маскировки вирусов привело к появлению следующих вирусов, которые классифицируются по технологии защиты от обнаружения [21]:

- шифрованный вирус – вирус, использующий простое шифрование своего тела со случайным ключом и неизменный шифратор. Такие вирусы могут быть обнаружены по сигнатуре шифратора;
- метаморфный вирус – вирус, применяющий метаморфизм ко всему своему телу для создания новых копий;
- полиморфный вирус – вирус, использующий метаморфный шифратор для шифрования тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм шифрования;
- стелс-вирус (stealth virus – вирус-невидимка) – вирус, полностью или частично скрывающий свое присутствие в системе путем перехвата обращений к операционной системе на осуществление чтения или записи в инфицированных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.) и подмены их содержимого с целью демонстрации подсистеме защиты оригинального содержимого объекта до его заражения.

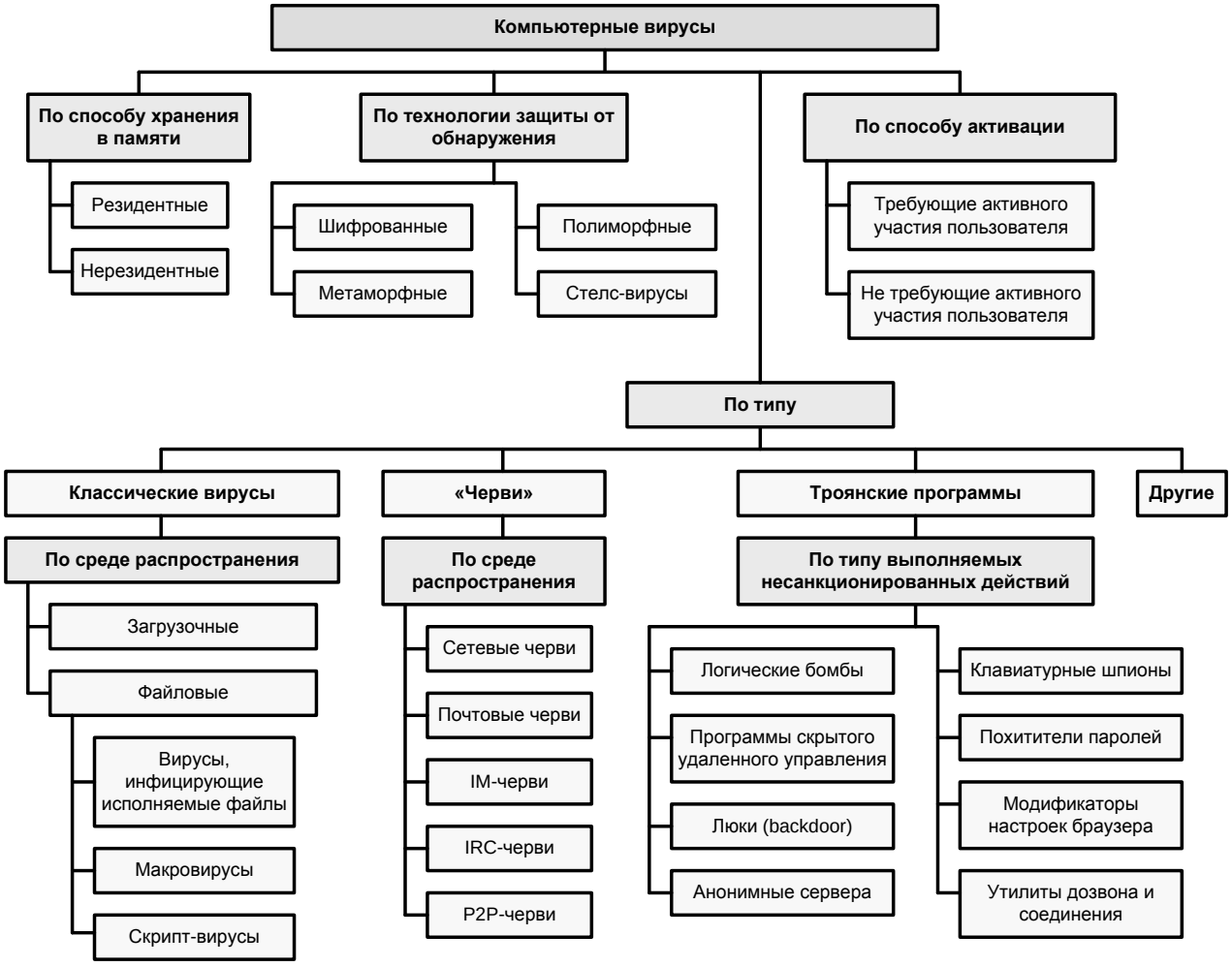


Рис. 7. Классификация компьютерных вирусов

Кроме того, компьютерные вирусы можно классифицировать по способу активации [21].

- Требующие активного участия пользователя. Отличительная особенность таких компьютерных вирусов является использование обманных методов. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добровольно открывает вложение с «почтовым червем», тем самым его активируя.
- Не требующие активного участия пользователя. Активация компьютерных вирусов без участия пользователя возможна за счет того, что вирус самостоятельно находит и использует уязвимости в безопасности информационной системы.

Общая схема классификации компьютерных вирусов представлена на рис. 7.

Рассмотрим основные особенности основных типов вирусов более подробно.

3.2.1 Классические вирусы

Основное свойство классического компьютерного вируса – это способность к саморазмножению [21].

Вирус – это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области операционных систем и прочие информационные ресурсы. При этом дубликаты сохраняют способность к дальнейшему распространению [21].

Условно жизненный цикл вируса можно разделить на пять стадий [21]:

- проникновение на чужой компьютер;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- внедрение копий;

Путями проникновения вируса могут служить мобильные носители, сетевые соединения, а также любые другие каналы, по которым можно скопировать файл. Однако в отличие от «червей», вирусы не используют сетевые ресурсы – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал [21].

После проникновения следует активация вируса. В соответствии с выбранным методом активации вирусы делятся на следующие виды [21]:

- загрузочные вирусы – заражают загрузочные сектора жестких дисков и мобильных носителей;
- файловые вирусы – заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют следующие типы вирусов:
    - вирусы, инфицирующие исполняемые файлы – различными способами внедряются в исполняемые файлы программ

(внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы;

- макровирусы – инструкции, написанные на внутреннем языке команд заражаемого приложения (на, так называемых, макросах);
- скрипт-вирусы – инструкции, написанные на внутреннем языке для определенной командной оболочки (скриптов).

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан [21].

Основная цель вируса – распространение на другие ресурсы информационной системы и выполнение деструктивных действий при определенных событиях или действиях пользователя [21].

3.2.2 Черви

В отличие от классических вирусов программы типа «червь» – это вполне самостоятельные программы, которые также способны к саморазмножению, однако при этом они способны и к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин «сетевой червь» [21].

Программа типа «червь» – это программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению подсистем защиты информационных систем, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом [21].

Жизненный цикл «червей» состоит из следующих стадий [21]:

- проникновение в информационную систему;
- активация;
- поиск объектов для заражения;
- подготовка копий;
- распространение копий.

В зависимости от способа проникновения в систему «черви» классифицируются на следующие типы [21]:

- «сетевые черви» – используют для распространения локальные сети, каналы в информационно-вычислительных сетях, глобальные сети, в том числе и Интернет;
- «почтовые черви» – распространяются с помощью почтовых программ;
- «IM-черви» – используют для распространения системы мгновенного обмена сообщениями типа Internet Massager;
- «IRC-черви» – распространяются по каналам IRC (Internet Relay Chat) для обмена информацией в чатах и форумах;
- «P2P-черви» – распространяются при помощи пиринговых P2P файлообменных сетей.

Сетевые черви могут кооперироваться с вирусами – такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса) [21].

3.2.3 Троянские программы

В отличие от вирусов и червей в программах типа «троянский конь» не всегда предусмотрен функционал саморазмножения. Довольно большая часть таких программ функцией саморазмножения вообще не обладает [21].

Программа типа «троян» («троянский конь») – программа, основной целью которой является вредоносное воздействие по отношению к информационной системе путем выполнения несанкционированных действий, а именно кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или несанкционированное использования его ресурсов [21].

Некоторые «трояны» способны к самостоятельному преодолению подсистемы защиты информационной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают в систему вместе с вирусом, либо с червем. В этом случае вирус или червь следует рассматривать как средство доставки, а «троян» – как средство информационного поражении [21].

Жизненный цикл «троянов» состоит всего из трех стадий [21]:

- проникновение в систему;
- активация;
- выполнение вредоносных действий.

Как уже говорилось выше, проникать в информационную систему «трояны» могут двумя путями – самостоятельно и за счет кооперации с вирусом или сетевым червем. В первом случае может быть использована маскировка, когда «троян» выдает себя за полезное приложение, которое пользователь самостоятельно копирует и запускает. При этом программа-носитель действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные «трояну» [21].

Для проникновения в информационную систему «трояну» необходима активация, и здесь он похож на «червя» – либо требует активных действий от пользователя, либо самостоятельно заражает ее, используя уязвимости в защите информационной системы [21].

Программы типа «троян», как правило, классифицируются по типу выполняемых несанкционированных действий [21].

- Логические бомбы – характеризуются способностью при выполнении заранее заложенных в них условий (конкретный день, время суток, определенное действие пользователя или команда извне) выполнять несанкционированные действия по уничтожению или искажению информации, воспрещения доступа к тем или иным важным фрагментам информационного ресурса, либо дезорганизации работы технических средств.
- Программы скрытого удаленного управления – это «трояны», которые обеспечивают несанкционированный удаленный контроль над

инфицированной информационной системой. Такие программы предоставляют удаленному пользователю возможность скрытого исполнения программ в информационной системе, поиска, модификации и удаления информации, возможности скрыто загружать или отсылать информацию.

- Люки (backdoor) – программы, находящие или создающие уязвимости в защите информационной системы с целью дальнейшего предоставления удаленного несанкционированного доступа к ней. От программ удаленного управления этот тип «трояна» отличаются более простой функциональностью и ориентированностью не на контроль системы, а на организацию доступа к ней. Как правило, данные «трояны» имеют функционал загрузки и запуска удаленных файлов. Это позволяет, при необходимости, загрузить на инфицированную систему программу скрытого удаленного управления и получить над информационной системой несанкционированный удаленный контроль.
- Анонимные сервера – разновидность «троянов», которые используют ресурсы зараженной информационной системы в своих целях, связанных с несанкционированной сетевой активностью: создание bot-сетей и управление ими, выполнение несанкционированных распределенных вычислений, организации и координация DDOS-атак, массовая отправка электронной почты, и другие подобные действия.
- Клавиатурные шпионы – находясь в оперативной памяти, записывают все данные, набираемые на клавиатуре с целью последующей их передачи.
- Похитители паролей – предназначены для кражи паролей и другой конфиденциальной информации путем поиска на зараженной системе специальных файлов, которые ее содержат.
- Модификаторы настроек браузера (программы просмотра информации в сети) – изменяют настройки браузера таким образом, чтобы стало возможным удаленное исполнение кода в браузере, доступ к хранящейся в нем конфиденциальной информации, подмена сертификатов безопасности, перенаправление на ложные страницы и т.п.
- Утилиты дозвона и соединения – в скрытом от пользователя режиме инициируют несанкционированное подключение к удаленным сервисам в сети.

Отдельно отметим, что существуют программы из класса «троянов», которые наносят вред другим, удаленным информационным системам и сетям, при этом, не нарушая работоспособности инфицированной системы. Примером таких программ могут служить анонимные сервера – организаторы DDoS-атак [21].

3.3 Программные закладки

Программная закладка – скрытно внедренная в защищенную информационную систему программа, либо намеренно измененный фрагмент программы, которая позволяет осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

При этом в большинстве случаев закладка внедряется самим разработчиком программного обеспечения для реализации в информационной системе некоторых сервисных или недекларируемых функций. Следовательно, под закладкой, как правило, понимается внутренний объект защищенной системы. Однако, в редких случаях, закладка может быть и внешним объектом по отношению к защищенной системе.

Программные закладки, получая несанкционированный доступ к данным в памяти информационной системы, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но в отличие от вирусов деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные. Довольно часто программные закладки выполняют роль перехватчиков паролей, сетевого трафика, а также служат в качестве скрытых интерфейсов для входа в систему. Однако, в отличие от вирусов, программные закладки не обладает способностью к саморазмножению, они встраиваются в ассоциированное с ними программное обеспечение и латентно функционируют вместе с ним. При этом, особенностью закладок, внедренных на стадии разработки программного обеспечения является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы [27].

Как и вирус, программная закладка должна скрывать свое присутствие в программной среде информационной системы. Однако программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами, выявляющими аномальное поведение и недекларируемые возможности программного обеспечения. В связи с этим, средства маскировки программных закладок преимущественно ориентированны на противодействие отладчикам программ, анализаторам кода и дисассемблерам. В качестве одного из широко применяемых способов маскировки является обфускация (запутывание) программ, в которые внедрена закладка [27].

Классификацию программных закладок можно провести по нескольким основаниям (рис. 8).

1. По месту внедрения в информационной системе программные закладки делятся на [27]:

- аппаратно-программные закладки, программно ассоциированные с аппаратными средствами (например, закладки в BIOS);
- загрузочные закладки, которые ассоциированы с программами начальной загрузки операционной среды информационной системы;

- драйверные закладки, которые ассоциированы с драйверами устройств информационной системы;
- прикладные закладки, которые ассоциированы с прикладным программным обеспечением общего назначения;
- исполняемые модули закладки, которые содержат только код программной закладки, который в дальнейшем внедряется в пакетные исполняемые файлы;
- закладки-имитаторы, имитирующие интерфейс служебных программ, работа с которыми предполагает ввод конфиденциальной информации;
- закладки, маскирующиеся под программы, позволяющие оптимизировать работу персонального компьютера, компьютерные игры и прочие развлекательные программы.

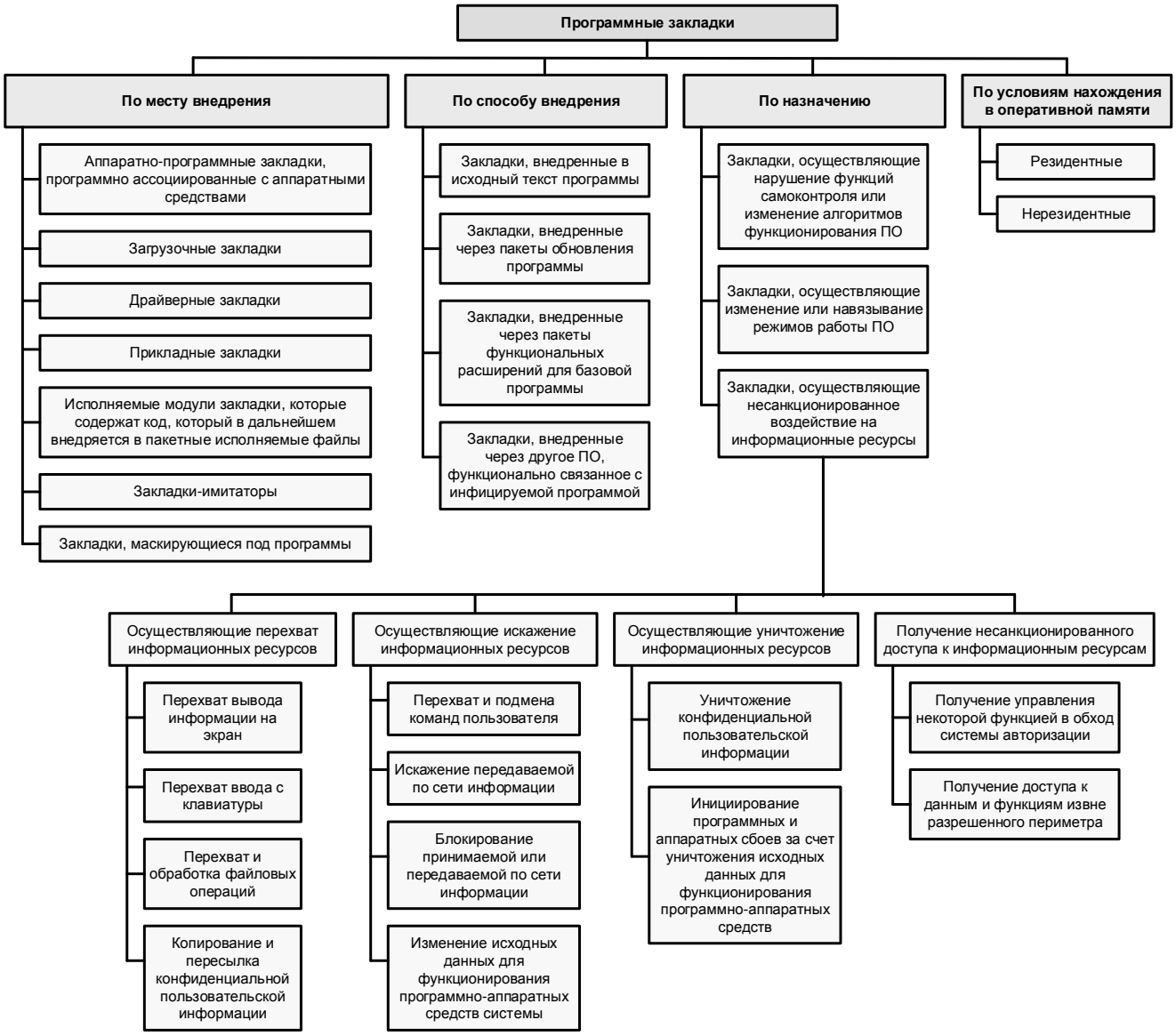


Рис. 8. Классификация программных закладок

2. По способу внедрения в программное обеспечение закладки можно классифицировать на:

- закладки, внедренные в исходный текст программы;
- закладки, внедренные через пакеты обновления программы;
- закладки, внедренные через пакеты функциональных расширений для базовой программы;
- закладки, внедренные через другое программное обеспечение, функционально связанное с инфицируемой программой;

3. По назначению программные закладки делятся на [27, 28]:

- закладки, осуществляющие несанкционированное воздействие на информационные ресурсы, которые находятся в оперативной или во внешней памяти системы, либо в памяти другой системы, подключенной по локальной или глобальной сети:
    - закладки, осуществляющие перехват информационных ресурсов:
        - перехват вывода информации на экран;
        - перехват ввода с клавиатуры;
        - перехват и обработка файловых операций;
        - копирование и пересылка конфиденциальной пользовательской информации;
    - закладки, осуществляющие искажение информационных ресурсов:
        - перехват и подмена команд пользователя;
        - искажение передаваемой по сети информации;
        - блокирование принимаемой или передаваемой по сети информации;
        - изменение исходных данных для функционирования программно-аппаратных средств системы;
    - закладки, осуществляющие уничтожение информационных ресурсов:
        - уничтожение конфиденциальной пользовательской информации;
        - инициирование программных и аппаратных сбоев за счет уничтожения исходных данных для функционирования программно-аппаратных средств;
    - получение несанкционированного доступа к информационным ресурсам:
        - получение управления некоторой функцией в обход системы авторизации;
        - получение доступа к данным и функциям извне разрешенного периметра;
- закладки, осуществляющие нарушение функций самоконтроля или изменение алгоритмов функционирования системных, прикладных и служебных программ;

- закладки, осуществляющие изменение или навязывание режимов работы программного обеспечения.

Для того, чтобы программная закладка начала функционировать, необходимо одновременное соблюдение двух условий, заставляющих систему исполнять команды, входящие в код программной закладки [27]:

- программная закладка должна попасть в оперативную память системы;
- должен быть выполнен ряд активизирующих условий, зависящих от типа программной закладки.

4. По условиям нахождения в оперативной памяти информационной системы программные закладки делятся на [27]:

- резидентные закладки, постоянно находящиеся в оперативной памяти до перезагрузки или завершения функционирования информационной системы;
- нерезидентные закладки, выгружающиеся из оперативной памяти информационной системы по истечении определенного времени, либо при выполнении определенных условий.

3.4 Аппаратные закладки

Аппаратная закладка – устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных средств информационной системы. Результатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение ее нормального функционирования, например несанкционированный доступ к информации, ее изменение или блокирование [29].

Также аппаратной закладкой может называться отдельная микросхема, несанкционированно подключаемая к атакуемой системе для достижения тех же целей [29].

Аппаратные закладки можно классифицировать по различным основаниям, следующим образом – рис. 9 [30].

1. По типу:
   - функциональная – закладка производится путем изменения состава аппаратных средств, добавлением или удалением необходимых элементов (например, транзисторов или логических вентилей в микросхеме);
   - параметрическая – закладка производится путем использования уже существующих компонентов аппаратного средства.
2. По расположению закладки:
   - в виде элементов микросхемы;
   - в отдельной микросхеме;
   - на электронной плате;
   - в аппаратных средствах информационной системы;
   - пространственно-распределенная по нескольким аппаратным средствам.

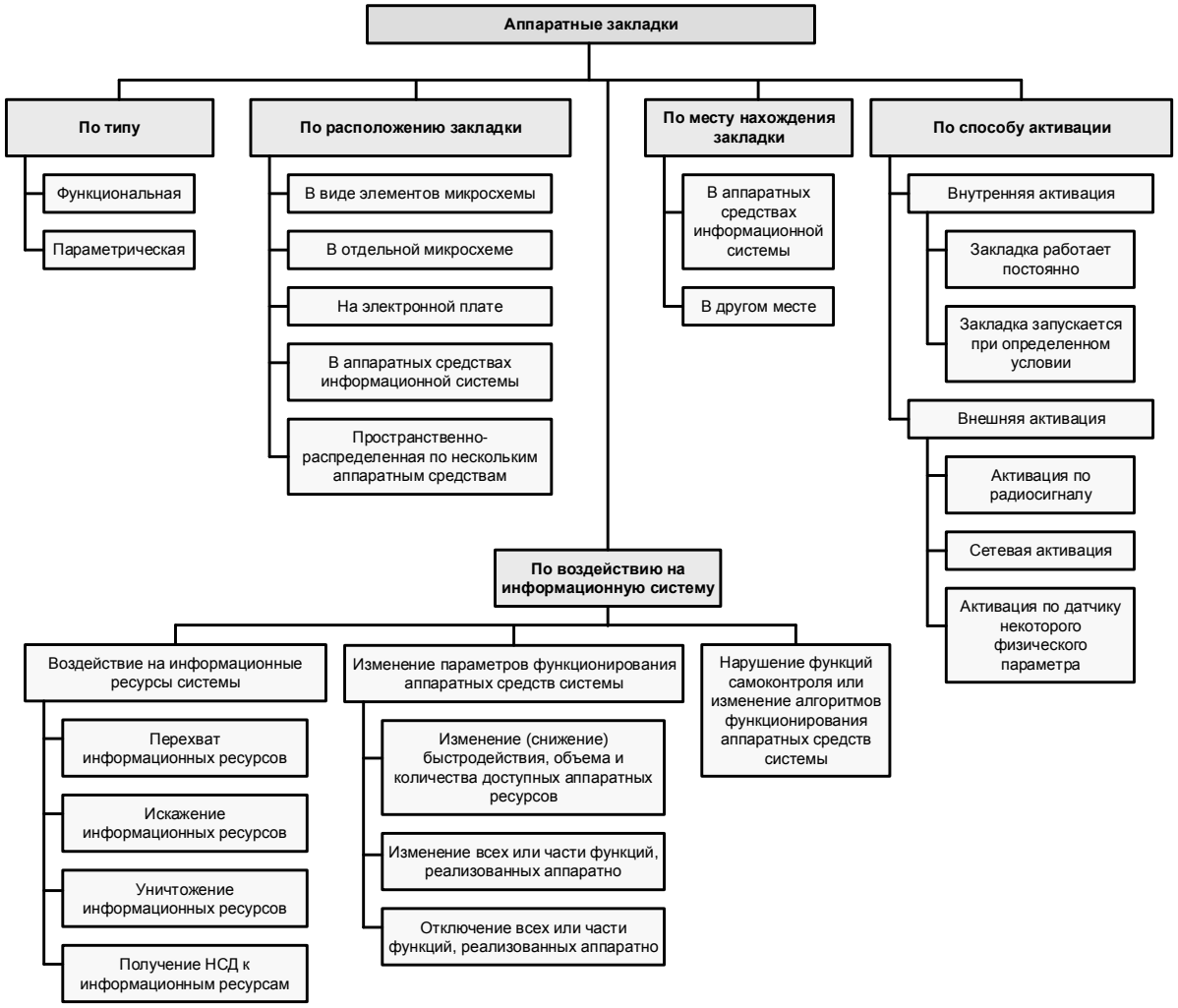


Рис. 9. Классификация аппаратных закладок

3. По объему – характеризует количество измененных, добавленных или удаленных элементов аппаратных средств, необходимых для внедрения закладки.
4. По месту нахождения закладки относительно ассоциированной информационной системы:
   - в аппаратных средствах информационной системы;
   - в другом месте.
5. По способу активации:
   - внутренняя активация:
     - закладка работает постоянно в составе аппаратного средства;
     - закладка запускается при определенном условии, заложенном при ее разработке;
   - внешняя активация – для запуска закладки используется внешний сигнал, который принимается антенной или датчиком:
     - активация по радиосигналу;
     - сетевая активация;
     - активация по датчику некоторого физического параметра.
6. По воздействию на информационную систему:
   - воздействие на информационные ресурсы системы:

- перехват информационных ресурсов;
- искажение информационных ресурсов;
- уничтожение информационных ресурсов;
- получение несанкционированного доступа к информационным ресурсам;

- нарушение функций самоконтроля или изменение алгоритмов функционирования аппаратных средств системы;
- изменение параметров функционирования аппаратных средств системы:
  - изменение (снижение) быстродействия, объема и количества доступных аппаратных ресурсов;
  - изменение всех или части функций, реализованных аппаратно;
  - отключение всех или части функций, реализованных аппаратно.

Схематическая сложность современного микроэлектронного оборудования, тенденции по миниатюризации его элементов ведут к тому, что производители оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, а при подключении устройств к глобальной сети – осуществлять обновление алгоритма их функционирования, а также условий срабатывания.

Краткая характеристика технологий современных аппаратных закладок представлена в таблице 1 [31].

Таблица 1 – Технологии современных аппаратных закладок [31]

Методы внедрения	Методы обнаружения	Методы маскировки
Встраивание закладок в технологию микроядра управления в современных СБИС, построенного на уникальном списке команд (управление основной работой и блокировка и замена неисправных узлов для продления срока службы СБИС)	Технологии послойного сканирования кристаллов	Механизм технологической защиты топологии кристалла от послойного сканирования (впервые внедрен в i486).
	Вычитывание и дизассемблирование аппаратно доступных микрокодов	Размещение микроядер с закладками и ресурсов памяти в области, не доступной пользователю. Шифрование (мутирование) участков кода, антитрассировка.
Виртуализация вычислений	Анализ контента проходящих по сети данных	
Встраивание целевых микроядер и узлов, реализующих стратегию влияния	Мониторинг аномальной активности платформы. Радио-мониторинг. Электромагнитный контроль.	

Достижения в области разработки и внедрения аппаратных закладок напрямую связанны с научным заделом в области микроэлектроники, а также с мощностями электронной промышленности. В настоящее время такие страны как США, Китай, Япония, в которых функционируют развитые производственные комплексы в области микроэлектронной и микропроцессорной техники, имеют потенциальную возможность встраивания аппаратных закладок в производимые ими на экспорт микроэлектронные компоненты. В дальнейшем это позволит контролировать функционирование подавляющей части АСУ технологическими и критическими процессами, а также средств радиоэлектроники в других странах. При этом в отношении этих стран может быть реализован сценарий мгновенного вывода из строя их критической инфраструктуры за счет одновременного отключения входящих в ее состав микроэлектронных компонентов.

В связи с этим можно выделить следующие риски использования импортных микроэлектронных компонентов при производстве систем управления войсками и оружием [31]:

- встроенная технологическая и схемотехническая избыточность микроэлектронных компонентов, превышающая необходимый уровень для предоставления сервисов по прямому назначению, позволяет внедрять в них недекларированные функции, в том числе и враждебного характера;
- отсутствие технической документации на топологии микросхем и логику функционирования не позволяет в полной мере провести эффективный технический контроль наличия закладок;
- отсутствие гарантированно подтвержденной надежности микроэлектронных компонентов, а также их стойкости к воздействию электромагнитного оружия, позволит противнику эффективно применять это оружие против систем управления войсками и оружием. При этом противник может создать электромагнитную обстановку, гарантирующую выход из строя им же произведенных микроэлектронных компонентов.

Образцом использования аппаратных закладок является обнародованная Э. Сноуденом информация о закладках Агентства национальной безопасности (АНБ) [32, 33, 34], использующихся для несанкционированного сбора данных в интересах разведывательных служб США. Практически все закладки были реализованы на аппаратном или аппаратно-программном уровне (при внедрении в перепрограммируемую память BIOS). Такое внедрение позволяет обеспечить функционирование закладки даже в случае обновления прошивки устройства или переустановки операционной системы, а кроме того, такая закладка слабо поддается обнаружению [33].

Другим ярким примером использования аппаратной закладки в военном конфликте является факт отключения системы иракской ПВО в военном конфликте в Персидском заливе в 1991 г. Тогда при проведении операции «Буря в пустыне» система ПВО Ирака оказалась заблокированной по неизвестной причине. Несмотря на отсутствие исчерпывающей информации по

этому инциденту, высказывалось предположение, что ЭВМ, входящие в состав системы ПВО, закупленные Ираком у Франции, содержали специальные управляемые «электронные закладки», блокировавшие работу вычислительных систем по внешней команде [27].

Такое действие закладки актуализирует вопросы обеспечения доверенной аппаратной среды при разработке электронных систем для критической инфраструктуры государства. Так как опыт локальных военных конфликтов показывает, что на первых этапах активных военных действий системы управления войсками и оружием, построенные на импортных компонентах, будут выводится из строя в первую очередь.

При этом в настоящее время фиксируются факты поставки в Вооруженные силы России вычислительной техники, которая фактически произведена иностранным изготовителем, снабжена разнообразными аппаратными закладками (например, одновременно в BIOS-е и сетевой карте компьютера), однако которая, пройдя перемаркировку и установку отечественного программного обеспечения считается де-юре «отечественного производства». При том, такие «отечественные производители», организующие подобные поставки, как правило, не имеют персонала должной квалификации для обнаружения и дезактивации встроенных в импортную технику аппаратных закладок, чем создают угрозу обороноспособности страны [35].

3.5 Нейтрализаторы тестовых программ и программ анализа кода

Одним из способов противодействия угрозам программных закладок является проверка программ, используемых в информационных системах управления критической инфраструктуры в процессе сертификационных испытаний и тематических исследований по требованиям безопасности [36, 37].

Сертификационные испытания и тематические исследования проводятся путем [36, 39]:

- функционального тестирования программного обеспечения на соответствие нормативным и методическим документам;
- структурного (статического и динамического) анализа программного обеспечения на отсутствие недекларированных возможностей.

При этом эксперты в области тестирования могут использовать дополнительные методы и приемы проверки кода, например: инспекция кода, использование статических анализаторов, изучение бюллетеней безопасности, организация стресс-тестирования и др.

При отсутствии исходных текстов программ применяются подходы реверс-инжинеринга и функциональные методы (по принципу «черного ящика»).

Реверс-инжиниринг может проводиться путем [36]:

- ретрансляции/дизассемблирования, прогона в отладочном режиме – для машинных и процедурных языков;
- высококачественной декомпиляцией – для языков с промежуточным кодом.

Сложность и размер современных программ таков, что для проведения сертификации используются специальные тестовые программы и анализаторы кода. Как правило, они ведут динамический анализ программного обеспечения, пока оно выполняется на реальном или виртуальном процессоре, фиксируя трассу управления, и формируемые потоки данных.

При использовании атакующих средств, например, таких как программная закладка, требуется обеспечить ее маскировку. В этом случае используется обеспечивающие средства – нейтрализаторы тестовых программ и программ анализа кода. Цель данных средств – затруднить анализ трассы исполнения программы и скрыть факт наличия закладки.

Средства нейтрализации тестовых программ и программ анализа кода используются либо на этапе компиляции исходного текста в машинный код, либо уже в процессе выполнения программы.

К основным способам нейтрализации тестовых программ относятся (рис. 10) [38, 39, 40]:

- обфускация (запутывание) кода;
- упаковка и шифрование кода;
- определение факта применения тестовых программ и противодействие отладке;
- полиморфизм (самомодифицирующийся код).

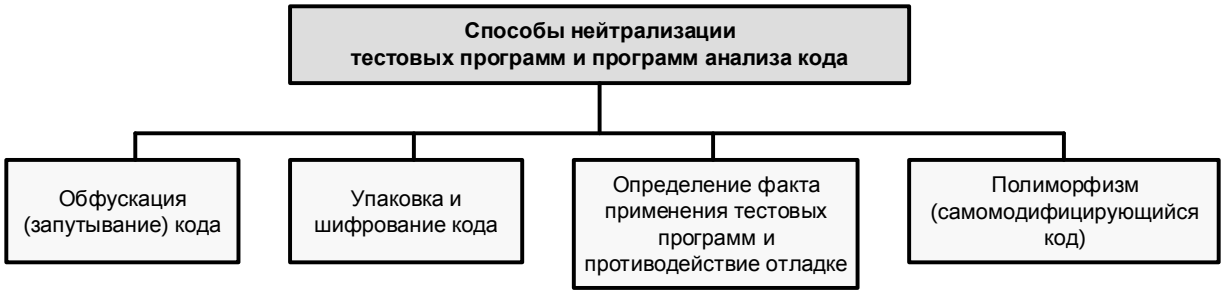


Рис. 10. Классификация способов нейтрализации программ

Рассмотрим данные способы более подробно.

Обфускация кода – приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ и понимание алгоритмов работы, а также модификацию при декомпиляции. Обфускация может осуществляться на различных уровнях: уровне алгоритма, уровне исходного текста, уровне машинного кода (ассемблерного текста). Кроме того, выделяют обфускацию на уровне виртуальных машин. Для создания запутанного машинного кода могут использоваться специализированные компиляторы, использующие неочевидные или недокументированные возможности среды исполнения программы. Существуют также специальные программы, производящие обфускацию, называемые обфускаторами [39].

Недостатками обфускации кода являются:

- код после обфускации может стать более зависимым от используемой платформы или компилятора;

- после обфускации дальнейшая отладка и тестирование программного кода становится невозможна;
- обфускация обеспечивает скрытие программных закладок через неясность программного кода, однако ни один из существующих обфускаторов не гарантирует устойчивости к определенному уровню сложности декомпиляции и не обеспечивает безопасности на уровне современных криптографических схем.

Упаковка и шифрование участков кода. При этом способе в программное обеспечение встраивается код шифратора и генератор ключей, после чего программа в процессе работы «на лету» дешифрирует инструкции машинного кода и передает их на исполнение. Использование такого способа противодействия тестовым программам позволяет существенно сузить их возможности по тестированию. Данный подход делает невозможным непосредственное дизассемблирование кода программы. Помимо этого, сохранение дампов памяти для последующего дизассемблирования становится крайне неэффективным, т.к. каждый дамп содержит только небольшой расшифрованный фрагмент программы [39].

Определение факта применения тестовых программ и противодействие отладке. Существует ряд приемов, позволяющих обнаружить выполнение тестирования и отладки. В случае обнаружения этого факта со стороны программы предпринимаются действия, направленные на противодействие исследованию за счет изменения логики своего функционирования:

- меняется работа алгоритмов;
- блокируется исполнение кода программы;
- «портятся» данные отладчика.

Такие способы противодействия отладке преодолеваются применением потактовых симуляторов. В этом случае обнаружение отладки возможно только из-за ошибок в симуляторе, приводящих к отличному от аппаратной платформы поведению [39].

Полиморфизм – генерация различных версий машинного кода для одного и того же алгоритма. Технология полиморфной генерации машинного кода позволяет проводить запутывающие преобразования защищаемого программного обеспечения. Для этого производится встраивание дополнительных или незначащих инструкций в защищаемый код, перестановка последовательности выполнения инструкций. Как правило, на этапе компиляции в программное обеспечение добавляется полиморфный генератор, который в процессе функционирования программы проводит модификацию ее машинного кода [40]:

- перестановка, обмен местами инструкций, порядок следования которых неважен;
- добавление «мусорных команд»;
- введение незначащих переменных;
- изменение процедуры самомодифицирования и др.

3.6 Средства создания ложных объектов информационного пространства

При защите информационных систем большое внимание уделяется вопросам обнаружения и нейтрализации уязвимостей входящего в их состав программного обеспечения (ПО). В настоящее время все основные способы решения данной задачи основываются на применении «стратегии запрета». Для этого в ручном или автоматизированном режиме проводится поиск уязвимостей ПО информационной системы, информация о которых имеется в открытых или закрытых базах данных. После обнаружения уязвимость нейтрализуется либо за счет обновления ПО, либо за счет использования средств защиты информации, таких как межсетевые экраны, системы обнаружения вторжений, средства антивирусной защиты и т.д., которые делают невозможным эксплуатацию данной уязвимости для реализации несанкционированного доступа [41].

Однако, как показывает практика, такая стратегия оказывается неэффективной против уязвимостей «нулевого дня». Это связано с тем, что между выпуском ПО и появлением информации об уязвимости, а тем более устранением ее разработчиками, в большинстве случаев проходит большое количество времени, в течение которого система оказывается уязвимой. Несмотря на то, что правильно настроенные средства защиты информации делают эксплуатацию некоторых из таких уязвимостей невозможной, всегда остается вероятность наличия не устраненных уязвимостей, а также уязвимостей в ПО самих средств защиты [41].

В связи с этим в настоящее время актуальным становится применение «стратегии обмана» или отвлечения атаки информационного оружия на ложный информационный ресурс. Как показали исследования [42], реализуя «стратегию обмана» атакующей системы и отвлекая атаку на ложный информационный ресурс, можно не только не позволить получить несанкционированный доступ к защищаемой информации, но и провести ответную информационную атаку – дезинформировав атакующую сторону. Кроме того, в период отвлечения атаки на ложные информационные ресурсы возможен сбор данных об атакующей стороне для компрометации последней.

В общем случае можно выделить два типа ложных ресурсов, ориентированных на различные сферы информационного противоборства:

- ложные объекты и ресурсы в семантической части информационного пространства (например, дезинформация или заведомо ложная информация, размещаемая в СМИ и в сети Интернет);
- ложные объекты и ресурсы в телекоммуникационной части информационного пространства (например, ложные сети, узлы, БД и т.д.).

Ложные объекты и ресурсы, размещаемые в семантической части информационного пространства, ориентированы на ведение информационного противоборства в психологической сфере и направлены, главным образом, на обеспечение информационно-психологических операций.

Ложные объекты и ресурсы в телекоммуникационной части информационного пространства ориентированы на ведение информационного противоборства в технической сфере. Они предназначены для обмана и отвлечения на себя атакующих информационно-технических воздействий.

К ложным объектам и ресурсам в телекоммуникационной части информационного пространства, на которые возможно эффективное отвлечение проводимых противником атак, можно отнести:

- узлы телекоммуникационных сетей;
- вычислительные и информационно-управляющие системы;
- операционные системы;
- прикладное программное обеспечение;
- базы данных и системы управления ими;
- программы управления контентом сайтов, новостных агрегаторов, страниц во внутренней сети или в сети Интернет.

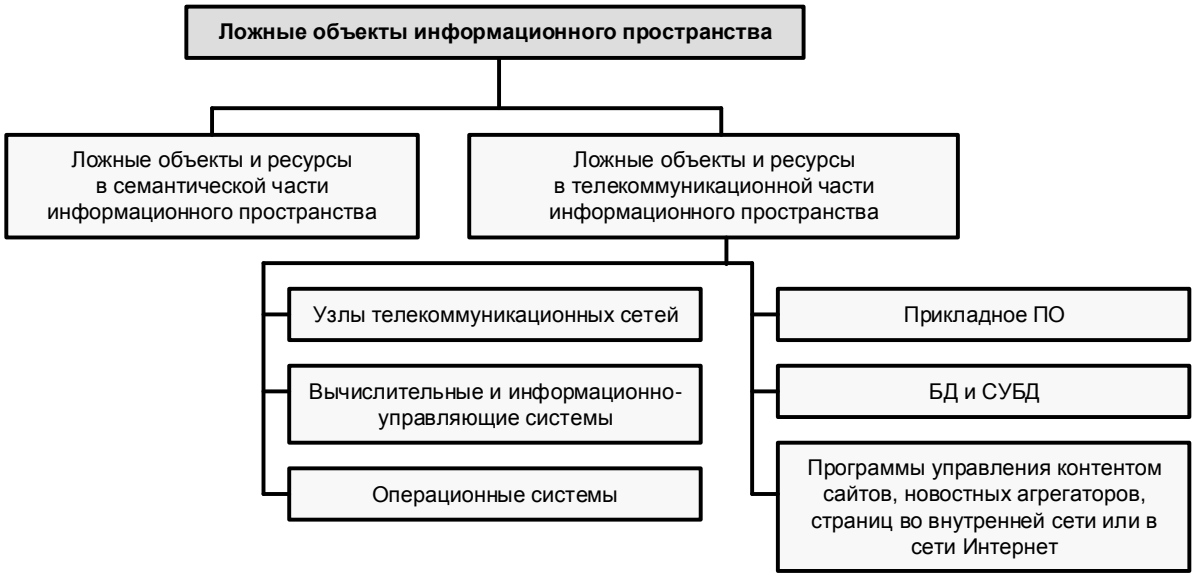


Рис. 11. Классификация ложных объектов информационного пространства

В качество средств создания и использования ложных объектов в телекоммуникационной части информационного пространства можно рассматривать программное обеспечение на основе технологий виртуализации. Такие программные средства виртуализации, как VMware ESX/ESXi, Microsoft Hyper-V, Citrix Xen Server и др., позволят создать виртуальную инфраструктуру, наполнить ее ложными объектами, содержащими дезинформацию и впоследствии управлять такой системой [41].

Кроме вышеуказанных средств виртуализации возможно использование других способов и средств создания ложных объектов. К ним можно отнести – создание ложных сетей путем подмены адресов объектов сети, развертывания дополнительных сетей с организацией по ним дезинформирующего информационного обмена, использование в сети средств защиты со специально введенными в них уязвимостями (так называемых «приманок»). С примерами

подобных решений можно ознакомиться в работах отечественных специалистов [60, 61, 62].

3.7 Средства моделирования боевых действий

Анализ вооруженных конфликтов свидетельствует о том, что успех сопутствует стороне, проявляющей большую активность и инициативу, эффективно управляющей подчиненными силами и средствами. Эволюционный путь развития автоматизированных средств управления войсками и оружием привел к разработке и принятию концепции создания системы моделирования военных действий [43].

В связи с развитием современных супер-компьютерных технологий уже в ближайшее время можно ожидать появления достаточных вычислительных возможностей для моделирования боевых действий с приемлемой степенью адекватности. Средства такого моделирования основаны на манипулировании информацией о составе, формах и способах действий войск (сил). Использование средств моделирования боевых действий позволят точно выбрать оптимальную стратегию действий при заданном составе группировки своих сил и средств, выбрать оптимальную траекторию развития противоборства с учетом вероятных действий противника и тем самым обеспечит подавляющее ассиметричное информационное превосходство над противником, при условии отсутствия у него подобных средств. При противоборстве двух сторон, обладающих подобными средствами, может создаться ситуация, что конфликт закончится еще в угрожаемый период. Когда сторона, которая по результатам моделирования не сможет найти выигрышной стратегии, самостоятельно признает себя проигравшей.

Вышеуказанные факты, а именно – использование средств моделирования боевых действий для достижения информационного превосходства над противником за счет обработки информации, позволяет отнести данные средства к информационному оружию.

Начиная с 70-х годов моделирование становится обязательным инструментом военных исследований. Широкое развитие получают имитационные модели, которые находят применение в военном планировании. В 80-е годы модели становятся повседневным рабочим инструментом в военном планировании, в непосредственном обеспечении деятельности руководства Вооруженных сил (ВС). Унифицируется информационное обеспечение моделей (базы данных). Проектируются иерархические системы моделей боевых действий различного уровня. Все более широкое распространение получает использование моделей в АСУ военного назначения. В ходе учений ACE-89 в Германии впервые реально была задействована система, объединившая модели различных уровней (DWS - Distributed Wargaming System). 90-е годы характеризуются еще более масштабными проектами внедрения моделирования в повседневную деятельность с охватом всех видов ВС США. Были созданы органы, обеспечивающие централизованное руководство разработкой и применением моделирования МО

США, координацию соответствующих работ как между видами ВС, так и в рамках какого-либо одного из направлений применения моделирования. Совершенствование средств имитации и моделирования в этот период ведется по пути интеграции моделей между собой и с состоящими на вооружении ВВТ, а также в направлении увеличения числа военнослужащих, выполняющих учебно-боевые задачи с использованием тренажерных комплексов. Значительно возросло количество учений различного уровня с использованием автоматизированных систем моделирования боевой обстановки. С середины 90-х годов командование американских ВС начало использовать новую форму проведения маневров – компьютерные учения с ограниченным привлечением войск и штатного ВВТ [45].

С начала 2000-х годов Пентагон при формировании военно-технической политики включил средства имитации и моделирования боевых действий в число приоритетных технологий. С начала 2000-х годов военное руководство США выделяет средства имитации и моделирования боевых действий в число приоритетных технологий при формировании военно-технической политики. Высокая динамика развития вычислительной техники, технологий программирования, системотехнических основ моделирования различных реальных процессов обозначили огромный прорыв США в области разработки моделей и имитационных систем [44, 45].

В настоящее время в министерстве обороны США действует классификация, определяющая назначение модели, объекты и процессы, метод моделирования (рис. 12) [45].

По назначению американские специалисты также выделяют три группы моделей [45]:

- используемые в целях анализа и оценки (обеспечение оперативной работы);
- применяемые в сфере создания ВВТ;
- предназначенные для обучения личного состава, обеспечения боевой подготовки войск и штабов.

В последнее время в ряде официальных документов военного ведомства предлагается более подробное подразделение моделей с выделением семи функциональных сфер моделирования [45]:

- оценка эффективности действий формирований в самостоятельных, совместных и объединенных операциях видов и родов сил;
- доктринальные исследования (военно-научные исследования и разработка концепций в области строительства ВС и их боевого применения);
- боевое обеспечение или поддержка операций (разведка, РЭБ и др.);
- создание ВВТ (снижение стоимости новых образцов и сокращение времени их создания, включая сферу НИОКР и закупок);
- испытания и оценка (потребностей ВС, повышение качества принимаемых решений в сфере планирования и разработки бюджетных программ, оценка эффективности новых образцов ВВТ);
- тыловое обеспечение;

- боевая подготовка и обучение личного состава.

При этом в последнее время акцент делается на создание систем моделирования, направленных на решение задач в области строительства и применения объединенных и коалиционных группировок войск (сил).

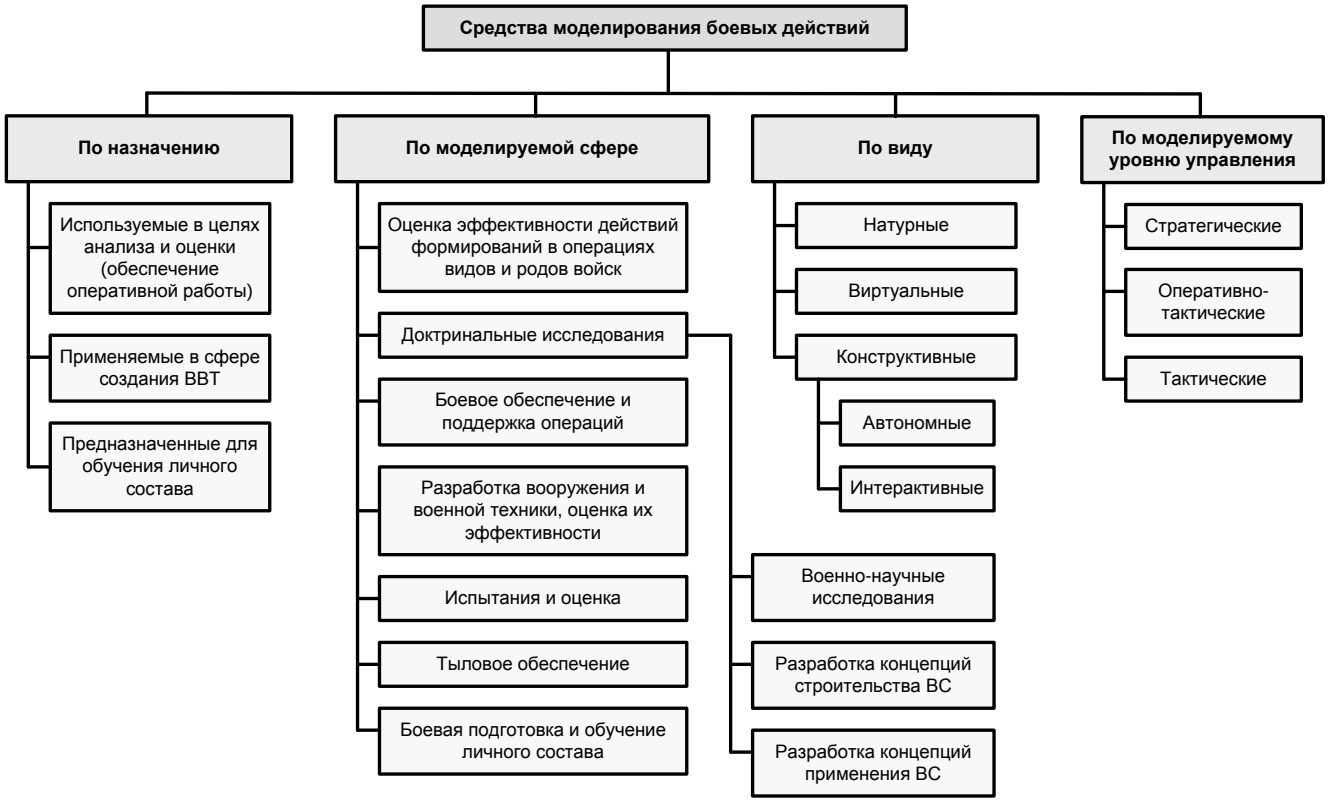


Рис. 12. Классификация средств моделирования боевых действий

Научно-технический совет МО США с начала 90-х годов ввел свой вариант классификации моделей, выделив три основные их вида, подчеркивая различие в степени и характере участия человека в процессе моделирования [45]:

- натурные;
- виртуальные;
- конструктивные.

К натурным системам относятся традиционные войсковые и командно-штабные учения с привлечением штатной техники и личного состава. В настоящее время отмечается тенденция к сокращению масштабов натурного моделирования и, напротив, расширяется использование других видов моделирования и имитации, особенно это касается виртуальных систем [45].

Виртуальные системы представляют собой человеко-машинные системы, в которых совмещается натурное и компьютерное моделирование. В первую очередь – это различные тренажеры ВВТ, применяемые для обучения. В настоящее время в большинстве виртуальных систем некоторые из компонент представлены в натурном виде, например реальными образцами вооружения и военной техники, а также обслуживающим их персоналом. В качестве весьма

перспективной разновидности виртуальной имитирующей системы может рассматриваться концепция так называемого виртуального прототипа. В таких системах предполагается полная замена реального оборудования его компьютерной имитацией. Данный подход широко используется при создании систем ВВТ [45].

Конструктивные системы могут быть [45]:

- полностью автономными (процесс моделирования не требует участия человека),
- интерактивными человеко-машинными системами.

Большинство используемых моделей являются именно конструктивными. Здесь предметная область, характерные для нее объекты и процессы представляются с помощью математического (алгоритмического) описания и соответствующего программного обеспечения. Термин применяется главным образом, чтобы подчеркнуть отличие этого класса моделей от натурных и так называемых виртуальных моделей. К конструктивным системам относятся разного рода имитационные модели [45].

Архитектура современных систем моделирования боевых действий стандартизирована. Она включает библиотеки стандартных программных модулей – генерирования случайных чисел, форматирования специфических докладов, выполнения сложных математических вычислений, управления ходом моделирования и др. [45].

Продолжаются работы по развитию объектно-ориентированной архитектуры моделей, призванной обеспечить более эффективное взаимодействие моделей и их использование. Такая архитектура позволяет создать инфраструктуру моделирования, которая может быть многократно использована в рамках разработки множества проектов создания моделей. При этом потребуется лишь добавить новую функциональность, реализующую решение новой задачи (описание новой среды функционирования или концептуальной схемы реального мира). По расчетам американских специалистов в этой области, возможно сокращение времени разработки моделей на 90% [45].

Важным направлением деятельности Министерства обороны США в сфере военного моделирования является оценка, подтверждение и сертификация моделей. Данные процедуры предполагают установление степени соответствия моделей процессам реального мира, а также установление применимости модели для решения специфических задач. Тем самым очерчиваются круг проблем или специфические условия существования проблем, для решения которых применима данная модель [45].

Основные направления модернизации объединенных систем моделирования и имитации боевых действий связаны в первую очередь с необходимостью создания новых моделей, а также с совершенствованием существующих систем. Дефицит моделей, вызванный динамизмом и глобальностью изменений в мире, а также появлением новых предметных областей, в значительной степени преодолен за последние годы. Тем не менее актуализация исследований применения ВС США в локальных конфликтах и в

различного рода «невоенных» операциях, например, при осуществлении миротворчества в борьбе с терроризмом, наркобизнесом и т. п., требуют разработки таких моделей, в которых был бы отражен значительно расширившийся спектр возможного применения Вооруженных сил. Требуются новые или уточненные модели для использования в следующих предметных областях: системы управления и связи; вычислительные системы и разведка; применение систем ПРО; радиоэлектронная борьба; применение оружия нелетального воздействия; роботизированные комплексы и системы; специальные операции; миротворческие операции; борьба с терроризмом и наркобизнесом и другие [45].

Высказывается мнение, что для нового поколения моделей требуется более полный учет взаимодействия многих военных, политических, экономических, этнических, религиозных и некоторых иных факторов, так или иначе влияющих на глобальную и региональную безопасность в современных условиях [45].

Перспективы развития моделирования связываются с развитием таких ключевых направлений развития науки и технологий, как: высокопроизводительные вычисления; компьютерные сети; визуализация; системы виртуальной реальности; распределенные системы моделирования. Благодаря программе Министерства обороны США по высокопроизводительным вычислениям ресурсы суперкомпьютеров становятся все более доступными для имитации через облачные вычислительные ресурсы [45].

В целом необходимо отметить, что развитие систем моделирования и имитации в США рассматривается как один из основных факторов обеспечения эффективности строительства и применения Вооруженных сил. Громадный потенциал, накопленный в данной области, уже сейчас оценивается как значительно опережающий возможности других стран мира в этой сфере [44].

В перспективе ожидается дальнейшее глобальное комплексирование моделей и внедрение систем виртуальной реальности (искусственного многомерного боевого пространства) на базе телекоммуникационных сетей, призванных обеспечить доступ пользователей как к оперативной, так и к физической моделируемой среде, к стандартизированным моделям и базам данных, а также к различного рода сценариям. Перспективные системы моделирования боевых действий будут имитировать применение вооруженных сил на любом континенте, на море, в воздухе и космическом пространстве, весь спектр их задействования (включая миротворческие операции, борьбу с терроризмом и т. п.). В будущем такие системы смогут с высокой степенью адекватности моделировать действия на фоне искусственно созданной боевой обстановки, воспроизводящей особенности любого театра военных действий (ТВД). А в качестве противника будут выступать как полностью, так и частично компьютеризированные «аналоги» реальных войсковых формирований [44].

Более подробная информация о подходах к моделированию боевых действий представлена в работе [46]. А примеры реальных средств

моделирования боевых применяемых в США в настоящее время – в работах [44, 45]. Кроме того, в работе [43] рассмотрен вариант подобного комплекса, разработанного специалистами республики Беларусь.

3.8 Средства технической разведки

Средства технической разведки предназначены для несанкционированного доступа к информации, ее копирования, а также преодоления подсистем защиты информации у технических и компьютерных систем противника. В связи с этим, с полным основанием их можно отнести к одному из видов обеспечивающего информационно-технического оружия. Средства технической разведки позволяют получить информацию об атакующих средствах информационно-технического оружия противника и способах его применения, что позволяет более рационально сконфигурировать собственные средства информационно-технической защиты. Воздействие средств разведки проявляется как в виде пассивных действий, направленных на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

Далее кратко рассмотрены средства основных видов технической разведки, при этом более полную информацию по этим средствам можно получить в фундаментальных работах в этой области – [47, 63, 64].

Техническая разведка – целенаправленная деятельность по добыванию с помощью технических средств соответствующих сведений в целях обеспечения военно-политического руководства своевременной информацией по разведываемым странам и их вооруженным силам [47].

Доля технической разведки в общей системе добывания защищаемой информации достаточно велика и, по некоторым оценкам, может составлять до 50% и более. Причем дальнейшее развитие науки и техники объективно приводит к повышению роли и значимости технической разведки [49].

При анализе технических средств разведки используют различные классифицирующие признаки.

1. По месту размещения технические средства разведки подразделяют на:
   - космические;
   - воздушные;
   - наземные;
   - кибернетические (размещаемые в информационном киберпространстве).

Для разведки используются различные каналы утечки информации, которые по основанию используемой физической среды (поля) классифицируются на [48, 49]:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (звуковые колебания в звукопроводящей среде);
- электрические каналы (напряжения и токи в токопроводящих коммуникациях);

- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой частях спектра);
- материально-вещественные каналы (бумага, фото, магнитные носители, отходы, выбросы и т.д.);
- другие каналы (радиационные, магнитометрические, сейсмические и т.д.);

2. В соответствии с классификацией каналов утечки информации выделяют следующие *виды технической разведки*, которые используют соответствующие средства [47, 48]:

- радиоэлектронную;
- оптическую;
- оптико-электронную;
- акустическую;
- гидроакустическую;
- химическую;
- радиационную;
- сейсмическую;
- магнитометрическую;
- компьютерную;
- измерительно-сигнатурную.

Классификация средств технических разведок приведена на рис. 13.

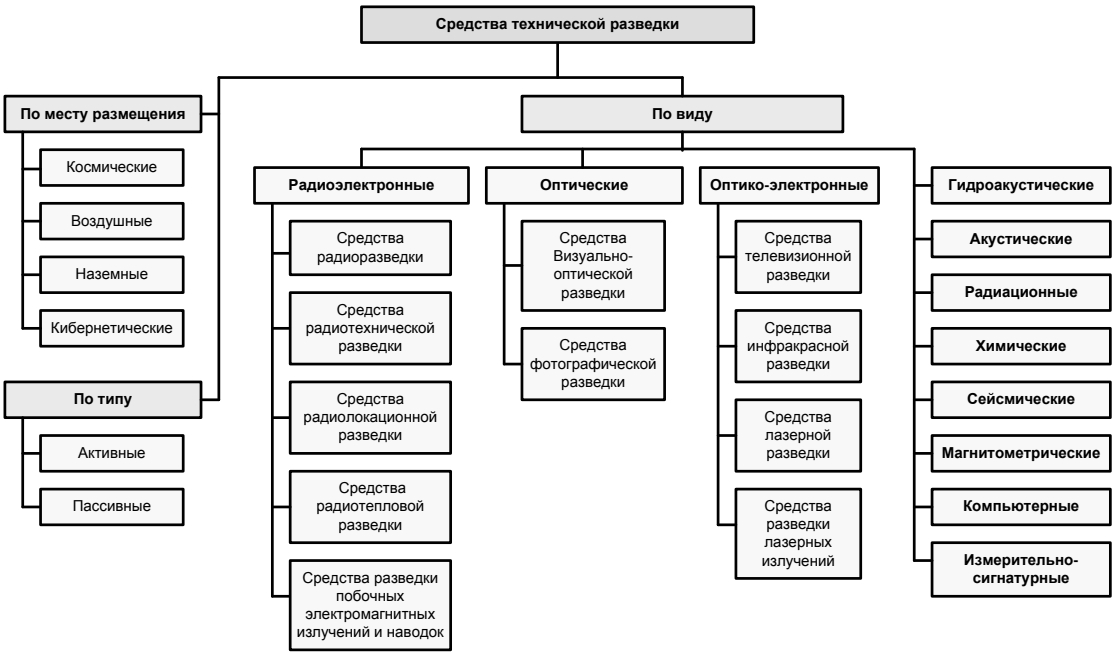


Рис. 13. Классификация средств технической разведки [50]

Рассмотрим данные виды разведок и соответствующие им технические средства более подробно на основании материала, представленного в работах [47, 63, 64].

Радиоэлектронная разведка (РЭР) – это процесс получения информации в результате приема и анализа электромагнитных излучений (ЭМИ) радиодиапазона, создаваемых работающими РЭС [47].

ЭМИ, создаваемые объектами разведки, могут быть первичными (собственными) или вторичными (отраженными) [47].

РЭР позволяет решать следующие задачи [47]:

- обнаруживать объекты, определять их местоположение и параметры движения;
- определять параметры объектов и характер их изменения во времени;
- определять назначение объектов и их типы;
- перехватывать передаваемую по каналам связи информацию.

Средства РЭР работают в пассивном или активном режиме (без излучения электромагнитных волн или с излучением) в широком диапазоне спектра радиочастот [47].

Радиоэлектронная разведка, в зависимости от ее целевого назначения, подразделяется на стратегическую и тактическую.

Стратегическая РЭР ведется в интересах правительственных органов и высшего военного командования с целью добывания всесторонней информации о разведываемой стране через его радиоэлектронные средства. Такая информация необходима для подготовки вооруженных сил и ресурсов страны к войне, принятия решения о начале военных действий и умелого ведения стратегических операций [47].

Тактическая РЭР считается одним из основных видов обеспечения войск информацией путем непрерывного слежения за электромагнитным излучением многочисленных военных устройств и систем противника. Она в состоянии добывать важные сведения для ведения боевых действий силами соединений, частей и подразделений [47].

Различают наземную, морскую, воздушную и космическую радиоэлектронную разведку. По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.

Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся [47]:

- открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи;
- тактико-технические данные и особенности разведываемых активных радиоэлектронных систем (частота настройки, вид модуляции и манипуляции, диаграммы направленности антенн, мощность излучения и т.п.), составляющие их «электронный почерк»;
- типы радиоэлектронных систем: радиосвязи, радиолокации, радионавигации, наведения ракет и дальнего обнаружения, различные телеметрические системы передачи данных;
- количество обнаруживаемых радиоэлектронных систем противника;
- местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемых разведываемой стороной впервые. Целью добывания технической информации является своевременная разработка

аппаратуры и методов радиоэлектронной разведки новых систем оружия и средств управления противника [47].

Для получения такой информации средствами РЭР ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками. При этом к наиболее важным источникам РЭР относятся:

- активные средства радиосвязи, используемые во всех видах вооруженных сил и в интересах управления государством;
- радиолокационные станции (РЛС) разных типов и назначений, применяемые, главным образом, в ПВО;
- автоматизированные системы управления, слежения и наведения ракетного и противоракетного оружия, а также космических объектов;
- радионавигационные системы, используемые в морской, воздушной и космической навигации;
- различные телеметрические системы передачи информации.

Радиоэлектронная разведка включает в себя следующие составные части [47]:

- радиоразведка;
- радиотехническая разведка;
- радиолокационная разведка;
- радиотепловая разведка;
- разведка побочных электромагнитных излучений и наводок.

Радиоразведка – самый старый вид радиоэлектронной разведки. Она ориентирована против различных видов радиосвязи. Основное содержание радиоразведки – обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций; пеленгование их сигналов; анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения; снижение нагрузки или подрыв криптографических систем [47].

Сведения радиоразведки о неприятельских станциях, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления, место размещения баз и стартовых площадок ракетного оружия и др.

Радиотехническая разведка (РТР) – вид разведывательной деятельности, целью которого является сбор и обработка информации, получаемой с помощью радиоэлектронных средств о радиоэлектронных системах по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах, смысловом содержании сигналов. Объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоуправления, радиотелекодовые системы, а также

ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т. п.) [47].

Средства РТР устанавливаются на самолетах, спутниках, кораблях, других объектах.

Радиолокационная разведка (РЛР) – вид технической разведки, в ходе которой информация добывается с помощью радиолокационных станций. РЛС могут быть стационарные наземные, переносные и установленные на самолетах, спутниках, кораблях, других мобильных объектах [47].

Радиотепловая разведка – вид разведывательной деятельности, целью которой является сбор информации о местоположении наземных, морских, воздушных и космических объектов по их тепловому излучению в радиодиапазоне. Характеристики радиотеплового излучения, такие как интенсивность и спектральный состав, зависят от физических свойств вещества и температуры объекта. Разведка ведется с помощью радиотеплолокационных станций, устанавливаемых на воздушных и космических платформах. Радиотепловая разведка возможна только при наличии контрастности теплового излучения объектов и фона (земной поверхности, неба и т.д.) [47].

Разведка побочных электромагнитных излучений и наводок – получение информации о передаваемой, обрабатываемой информации, а также информации об особенностях построения и функционирования технических средств путем анализа их побочных электромагнитных излучений и наводок от них.

Оптическая разведка – добывание информации с помощью оптических средств, обеспечивающих прием электромагнитных колебаний ультрафиолетового, видимого и инфракрасного диапазонов, излученных или отраженных объектами и предметами окружающей местности [47].

Оптическая разведка подразделяется на [47]:

- визуально-оптическую разведку;
- фотографическую разведку.

Оптико-электронная разведка (ОЭР) – процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и инфракрасного диапазонов, излученных или отраженных объектами и местностью [47].

ОЭР подразделяют на [47]:

- телевизионную разведку;
- инфракрасную разведку;
- лазерную разведку;
- разведку лазерных излучений.

Средства ОЭР устанавливаются на космических и воздушных носителях, а также могут применяться в наземных условиях, например, при ведении технической разведки [47].

Средства ОЭР делятся на [47]:

- пассивные;

- активные.

Пассивные основаны на приеме собственного или переотраженного излучения объектов разведки. Активные предполагают использование для подсвета местности собственного излучателя. Зондирующее излучение рассеивается объектами, местными предметами и местностью, часть этого излучения поступает на вход оптической системы аппаратуры разведки с последующим его преобразованием, обработкой и индикацией на соответствующих устройствах [47].

Средства пассивной ОЭР подразделяются на: телевизионные, инфракрасные и средства разведки лазерных излучений. Аппаратура телевизионной разведки охватывает устройства на ЭЛТ и на ПЗС. К средствам инфракрасной разведки относят тепловизоры, телепеленгаторы, радиометры и приборы ночного видения. Средства разведки лазерных излучений предназначены для обнаружения, определения местоположения и распознавания средств вооружения и военной техники, в состав которых входят лазерные излучатели [47].

Средства активной ОЭР подразделяются на [47]:

- лазерные со сканированием зондирующего светового луча;
- инфракрасные с использованием ИК-излучателя для подсвета местности.

Гидроакустическая разведка – получение информации путем приема и анализа акустических сигналов инфразвукового, звукового и ультразвукового диапазонов, распространяющихся в водной среде от надводных и подводных объектов [47].

По принципу использования энергии акустического излучения средства гидроакустической разведки делятся на активные (гидролокаторы) и пассивные [47].

Активные средства работают по принципу излучения в водной среде зондирующих акустических сигналов с последующим приемом и анализом отраженных от объектов и морского дна эхосигналов [47].

При ведении пассивной гидроакустической разведки используют шумопеленгаторы, которые принимают и анализируют шумовые акустические излучения в водной среде, возникающие при работе двигателей, гребных валов, машин и механизмов различных агрегатов надводных кораблей, подводных лодок и других плавсредств, а также средства разведки, предназначенные для приема и анализа акустических сигналов, создаваемых гидролокаторами, эхолотами, системами гидроакустической связи и др. [47]

Акустическая разведка – получение информации путем приема и анализа акустических сигналов инфразвукового, звукового, ультразвукового диапазонов, распространяющихся в воздушной среде от объектов разведки. Акустическая разведка обеспечивает получение информации, содержащейся непосредственно в произносимой либо воспроизводимой речи (акустическая речевая разведка), а также в параметрах акустических сигналов, сопутствующих работе вооружения и военной техники, механических

устройств оргтехники и других технических систем (акустическая сигнальная разведка) [47].

Радиационная разведка – получение информации в результате анализа радиоактивных излучений, связанных с выбросами и отходами атомного производства, хранением и транспортировкой расщепляющихся материалов, ядерных зарядов и боеприпасов, производством и эксплуатацией реакторов, двигателей и радиоактивным заражением местности [47].

Химическая разведка – добывание информации путем контактного или дистанционного анализа изменений химических свойств состава окружающей среды под воздействием выбросов и отходов производства, работы двигателей, в результате взрывов и выстрелов, преднамеренного рассеивания химических веществ, испытаний и применений химического оружия [47].

Сейсмическая разведка – добывание информации путем обнаружения и анализа деформационных и сдвиговых полей в земной поверхности, возникающих под воздействием различных взрывов [47].

Магнитометрическая разведка – добывание информации путем обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой [47].

Измерительно-сигнатурная разведка ведется в интересах обеспечения успеха военных операций вооруженных сил, создания новых поколений вооружения и военной техники, определения направлений модернизации вооруженных сил, контроля за распространением оружия, окружающей средой, а также выполнением военных договоров [47].

Сущность измерительно-сигнатурной разведки заключается в комплексном характере сбора разведывательной информации: во-первых, измерение геометрических размеров и соотношений статических, динамических и других физических характеристик разведуемых объектов (стационарных и подвижных) и, во-вторых, регистрация сигнатур характерных физических полей, создаваемых этими объектами (электромагнитных, магнитных, радиационных, акустических, сейсмических и других), а также выявление химических и биологических агентов и даже состава конструкционных материалов объектов и их элементов. При этом, используются все существующие датчики: оптические, радиолокационные, лазерные, радиочастотные, акустические, сейсмические, радиационные, химические, оптико-электронной и радиолокационной съемки с перекрытием практически всего спектра электромагнитных колебаний [47].

Следует иметь в виду, что физические измерения и снятие сигнатур не являются самоцелью измерительно-сигнатурной разведки. Главное в ней – выявление назначения, тактики применения, возможностей и основных характеристик, а также уязвимых мест разведываемого объекта [47].

Дополнительные сведения о средствах технической разведки, а также примеры конкретных технических устройств представлены в работах [47, 48, 63, 64].

3.9 Средства компьютерной разведки

Средства компьютерной разведки являются одним из видов средств технической разведки.

Под компьютерной разведкой традиционно было принято понимать получение информации из баз данных ЭВМ, включенных в компьютерные сети, а также информации об особенностях их построения и функционирования [47]. Однако, в настоящее время стало общепризнанным, что это слишком узкий, упрощенный подход к компьютерной разведке и в настоящее время данное понятие активно модернизируется и развивается.

Объектами компьютерной разведки являются компьютерные системы и сети, которые включают: отдельные ЭВМ, многопроцессорные ЭВМ и компьютерные системы, информационно-вычислительные сети, программно-аппаратные комплексы, программное обеспечение ЭВМ, периферийное компьютерное оборудование, различное оборудование, содержащее встроенные процессоры и микро-компьютеры и т.п. [51].

Таким образом, в наиболее общем случае под компьютерной разведкой понимается добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей. В связи с этим, выделяют три типа источников информации для компьютерной разведки [51]:

- данные, сведения и информация, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- характеристики программных, аппаратных и программно-аппаратных комплексов;
- характеристики пользователей компьютерных систем и сетей.

Классификацию средств и способов компьютерной разведки можно провести по нескольким основаниям (рис. 14).

По виду реализации средства компьютерной разведки можно разделить на:

- *физические* – реализованные в виде физических или аппаратных средств, которые подключаются к инфокоммуникационной инфраструктуре, ведут анализ физических полей, побочных электромагнитных излучений и наводок (ПЭМИН) в интересах добывания данных, сведений и информации;
- *программные* – реализованные в виде программных средств, которые в виде вирусов, закладок или специализированного программного обеспечения добывают данные, сведения и информацию за счет анализа логики построения и функционирования компьютерных систем, а также информационных потоков циркулирующей в них.

По принципам построения средств и их функциональному предназначению можно выделить следующие типы компьютерной разведки [51]:

- *семантическая* – обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа

структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;

- *алгоритмическая* – с использованием программно-аппаратных закладок и недекларированных возможностей, обеспечивающая добывание данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;
- *вирусная* – обеспечивающая добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и в системы для перехвата управления компьютерными системами;
- *разграничительная* – обеспечивающая добывание информации из отдельных компьютерных систем, возможно и не входящих в состав сети, на основе преодоления средств разграничения доступа, а также реализация несанкционированного доступа при физическом доступе к компьютерам, сетям или к компьютерным носителям информации;
- *сетевая* – обеспечивающая добывание данных из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий;
- *потоковая* – обеспечивающая добывание информации и данных путем перехвата, обработки и анализа сетевого трафика и выявления структур компьютерных сетей, а также их технических параметров;
- *аппаратная* – обеспечивающая добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки;
- *форматная* – обеспечивающая добывание информации и сведений путем «вертикальной» обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем – в информацию для последующего ее наилучшего представления пользователям;
- *пользовательская* – обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем

обеспечения им доступа к информации, циркулирующей в специально созданной ложной информационной инфраструктуре.

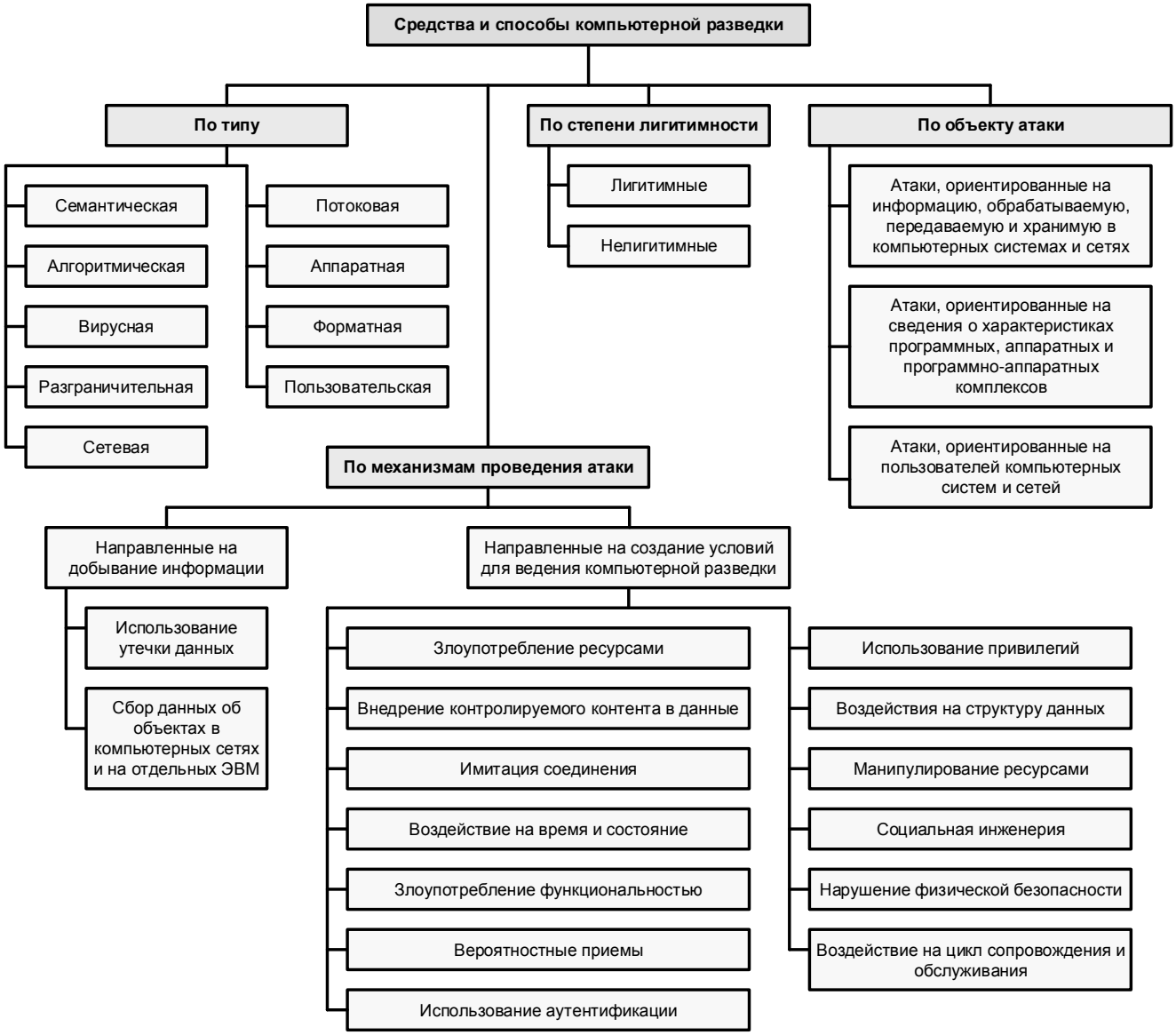


Рис. 14. Классификация средств и способов компьютерной разведки

На данном этапе развития компьютерных систем и сетей эти девять типов компьютерной разведки охватывают все существующие многоуровневые «горизонтальные» и «вертикальные» каналы утечки информации из компьютерных систем и сетей. При этом внутри указанных типов возможно выделение нескольких подтипов разведки, например, по виду добываемой информации на: фактографическую («видовую») и параметрическую.

Основным способом реализации разведки является атака средств компьютерной разведки [52, 53].

Под атакой средств компьютерной разведки будем понимать как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия,

направленные на создание условий благоприятствующих добыванию информации.

Атаки средств компьютерной разведки также можно классифицировать по различным основаниям.

По степени лигитимности атаки средств компьютерной разведки можно разделить на [52]:

- лигитимные (разведка на основе открытых источников, анализ сетевого трафика);
- нелигитимные (перехват трафика, несанкционированный доступ к компьютерным системам и т.д.).

По объекту атаки [51]:

- атаки, ориентированные на данные, сведения и информацию, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- атаки, ориентированные на сведения о характеристиках программных, аппаратных и программно-аппаратных комплексов;
- атаки, ориентированные на сведения о пользователях компьютерных систем и сетей.

По механизмам проведения атаки [53]:

- атаки, направленные на добывание информации в компьютерных сетях и ЭВМ:
    - использование утечки данных;
    - сбор данных об объектах в компьютерных сетях и на отдельных ЭВМ;
- атаки, направленных на создание благоприятных условий для ведения компьютерной разведки:
    - злоупотребление ресурсами;
    - внедрение контролируемого контента в данные;
    - имитация соединения:
    - воздействие на время и состояние;
    - злоупотребление функциональностью;
    - вероятностные приемы;
    - использование аутентификации;
    - использование привилегий;
    - воздействия на структуру данных;
    - манипулирование ресурсами;
    - социальная инженерия;
    - нарушение физической безопасности;
    - воздействие на цикл сопровождения и обслуживания.

Другие аспекты описания атак, такие как способы нападения и используемые уязвимости, также можно рассматривать в качестве оснований для классификации атак компьютерной разведки.

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества признаков. В научной литературе представлены различные классификации,

отличающиеся полнотой учета признаков. Наиболее полный учет признаков реализован в классификации CAPEC [54], разработанной корпорацией MITRE и применяемой для ведения базы данных образцов компьютерных атак в интересах защиты киберпространства США. Однако, классификация атак CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учитывая этот недостаток классификации CAPEC, отечественными специалистами в работе [53] была предложена классификация атак средств компьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 15.

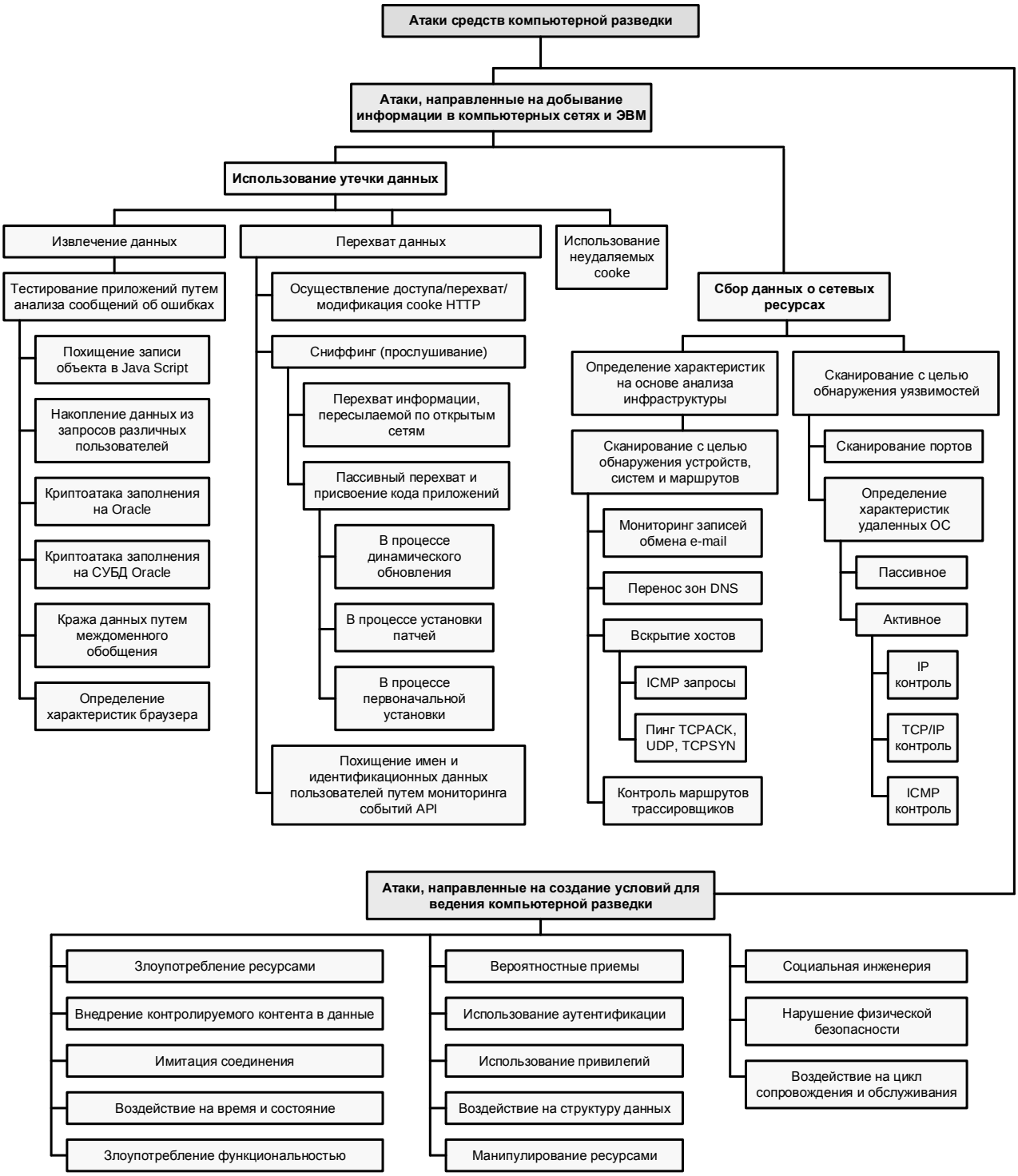


Рис. 15. Классификация атак компьютерной разведки [53]

В настоящее время многие технологически развитые страны активно разрабатывают и совершенствуют собственные средства и комплексы компьютерной разведки. Большинство программ по разработке таких комплексов санкционированы на государственном уровне и ведутся для получения стратегического информационного превосходства в военной, политической и промышленной сфере.

К странам, имеющим наибольшие достижения в области создания глобальных комплексов компьютерной разведки необходимо отнести США (программы: «Carnivore», «Eshelon», «NarusInsight», «Turbulence», «CO-TRAVELER», «PRISM», «Dropmire», «X-Keyscore»), Великобританию (программа «Tempora»), Китай (программа «Золотой щит») и Россию (программа «СОРМ»). Помимо них, другие технически развитые страны также создают свои комплексы компьютерной разведки – Франция (программа «Frenchelon»), Швейцария (программа «Onyx»), Швеция (программа «Titan»), Индия (программы «NATGRID», «Central Monitoring System», «DRDO NETRA»).

3.10 Средства разведки по отрытым источникам в глобальном информационном пространстве

Разведка на основе анализа открытых источников информации (Open Source Intelligence – OSINT) является достаточно старым видом деятельности для военной разведки США, и ее история ведется еще со времен Второй мировой войны. Однако, если ранее OSINT рассматривалась как возможность «закрывать информационные бреши» в случае неспособности других видов разведки выполнить поставленную задачу, то сейчас, в связи с развитием в начале XXI века глобального информационного пространства и сети Интернет, по оценкам американского военного руководства, OSINT резко повысила свою значимость [55, 56].

Во многом повышение значимости разведки на основе анализа открытых источников обусловлено тем фактом, что порядка 10-15% необходимой информации имеется в Интернете уже в готовом виде (необходима только ее верификация), а остальные 85-90% информации могут быть получены в результате сравнения, анализа и синтеза разрозненных и разбросанных по разным источникам фактов. Естественно, что информация, полученная таким образом, нуждается в верификации [57].

В сферу интересов такой разведки входит добывание и анализ официальных документов, проектов уставов и наставлений, отслеживание новых научных разработок и проектов, баз данных, коммерческих и государственных интернет-сайтов, сетевых дневников и многого другого [55, 56].

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа. Вариант классификации таких средств представлен на рис. 16.

Рис. 16. Вариант классификации
средств разведки по отрытым источникам

3.10.1 Средства разведки на основе традиционного семантического анализа и поисковых программ

В качестве средств разведки на основе анализа открытых источников в Интернете традиционно используются специальные программы анализа данных. Под ними понимаются программы-роботы, которые опрашивают сайты и извлекают из них нужную информацию, используя широкий спектр средств лингвистического, семантического и статистического анализа. Действуя автономно, такие программы анализа данных выявляют любую целевую информацию, как только она появится в Интернете [57].

Примерами таких программ могут служить программы «Taiga», «Tropes», «Noemic», «Info Tracer» [57].

В виду того, что имеющимися техническими средствами полностью формализовать процедуру поиска информации пока не представляется возможным, реализовать сложную стратегию поиска необходимой информации часто бывает весьма затруднительно. Поэтому при ведении разведки по открытым источникам в сети Интернет приходится идти по пути информационной избыточности, что накладывает весомые ограничения на релевантность найденных документов. Из-за высокого уровня информационного шума в общем объеме найденных документов значительно увеличивается время, необходимое для аналитической обработки полученных сведений [57].

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию, которая в явном виде находится в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с

совпадающим целевым контентом, начинают «собирать» информационное наполнение запроса пользователей. Более интересным направлением развития средств разведки является анализ разнородных, изначально семантически не связанных между собой, данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направление получило развитие в рамках исследования проблемы «Больших Данных» (Big Date).

3.10.2 Средства разведки на основе технологий «Больших Данных»

Термин «Большие Данные» был впервые введен в 2009 году в специальном выпуске ведущего американского научного журнала Nature, целиком посвященного этой теме. Введение этого понятия обусловлено следующими факторами.

1. Глобальная сеть Интернет перешла в фазу явно выраженного экспоненциального развития, или по другому – «информационного взрыва». Примерно с 2008 г. объем информации, вновь генерируемой в сети Интернет, стал удваиваться в течение, примерно, полутора-двух лет. При этом примерно треть передаваемых данных составляют автоматически сгенерированные данные, т.е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к глобальной сети, или как его называют – «Интернету вещей» [58].
2. В 2010-х годах появились и стали доступны принципиально новые IT-решения, позволяющие в режиме реального времени обрабатывать практически безразмерные массивы данных самого различного формата. Причем эти решения сразу же стали реализовываться не только как программные платформы, устанавливаемые на серверы, но и как облачные решения, при использовании которых от организации не требовалось наличия дорогостоящей компьютерной инфраструктуры [58].
3. В-третьих, к концу 2000-х годов западные поведенческие и когнитивные науки из фазы фундаментальных исследований перешли в стадию разработок эффективных технологий анализа поведения и социальных связей в обществе [58].

Таким образом, формирование глобального электронного, постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и огромных компаний до небольших групп и отдельных индивидуумов собственно и послужило базисом появления Больших Данных. С тех пор направление Больших Данных стало ведущим в сфере информационных технологий.

Анализ накопленного за последние годы опыта применения технологий Больших Данных позволяет выделить несколько ключевых черт, отличающих их от всех других информационных технологий. К ним относятся [58]:

- во-первых, огромные массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т.п., пополняемые непрерывно в режиме реального времени. Согласно имеющейся статистике, 60% этой информации носит неструктурированный, в основном текстовой характер и 40% – составляет структурированная, или табличная информация. В последние годы в общем объеме Больших Данных постоянно нарастает доля информации структурированного характера, поступающей от устройств, имеющих связь с Интернетом;
- во-вторых, специально спроектированные программные платформы, где Большие Данные любого объема могут храниться в удобном для обработке виде. Особо надо подчеркнуть, что эти архивы отличаются от стандартных баз данных. Отличительной чертой этих хранилищ является то, что структурированная и неструктурированная информация могут обрабатываться совместно, как единое целое;
- в-третьих, наличие различного рода математического, прежде всего, статистического инструментария для обработки Больших Данных и получение результатов в виде, понятном для человека. Причем, при анализе Больших Данных используются не только традиционные методы математической статистики, но и интеллектуальные алгоритмы обработки данных.

В соответствии с данными исследования [58], не более 0,6% информации, находящейся в Интернет, подпадает под категорию Больших Данных, т.е. накапливается, хранится и перерабатывается. В этом же исследовании указывается, что потенциально в качестве Больших Данных может использоваться порядка 23% всей хранимой в настоящее время информации.

Технологии Больших Данных основаны прежде всего на методах статистического и интеллектуального анализа данных, применяемых на огромных, постоянно пополняемых массивах данных. Эти технологии позволяют [58]:

- *проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам*. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации, с теми или иными его действиями;
- *осуществлять многомерный статистический математический анализ*. Этот анализ позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Корреляции не отвечают на вопрос – почему. Они показывают вероятность, с которой при изменении одного фактора изменяется и другой. В каком-то смысле Большие Данные представляют собой альтернативный традиционной науке метод познания действительности. Теоретические модели отвечает на вопрос – почему, а затем, выявив причинно-следственные закономерности, позволяют

формировать рекомендации о порядке действий. В случае выявления корреляционных закономерностей в Больших Данных, стадия выявления первопричины отсутствует, а сразу выявляется закономерная связь различных факторов. При этом, если факторы тесно взаимосвязаны, то на один из факторов возможно осуществить воздействие для достижения целенаправленного изменения связанного с ним фактора;

- *прогнозировать*. На основе классификаций и аналитических выкладок осуществляется прогнозирование, суть которого состоит в том, чтобы на основе выявленной корреляционной связи факторов определить наиболее целесообразный способ воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п. был преобразован в другой.

Большие Данные как прорывная информационная технология были быстро осознаны такими странами как США, Великобритания и Япония. 29 марта 2012 г. администрация Б. Обамы выступила с инициативой «Big Data Research and Development Initiative». Этой инициативой предусматриваются вложение значительных объемов ресурсов и проведение комплексных мероприятий в целях активного использования технологий Больших Данных в интересах ключевых направлений политики США [58].

Большие Данные, в первую очередь, были использованы в маркетинге, инвестиционном бизнесе, в продажах и т.п. В дальнейшем технологии Больших Данных стали использоваться в таких сферах как разведка и контрразведка, военное дело, геостратегия, а также в информационном противоборстве [58].

Помимо непосредственно разведки и контрразведки, технологии Больших Данных начали использоваться для выявления глубоких паттернов поведении в социальной среде.

В последние годы создана, по сути, новая наука – социодинамика, которая обобщает эмпирические закономерности, полученные в результате применения технологий Больших Данных к огромным массивам информации, содержащейся в архивах крупнейших социальных платформ на основе Web и Web 2.0, таких как Google, Facebook, Twitter и т.п. Эти эмпирические закономерности сегодня используются для отработки практического инструментария внешнего воздействия, управления и манипулирования социальными группами любых масштабов и любого уровня структурированности, а также для сборки и деструкции социальных субъектов. Именно применение Больших Данных к информации, полученной из социальных сетей, позволило осуществить прорыв в отработке инструментария внешнего социального управления поведением [58].

3.10.3 Средства прогнозирования на основе технологий «Больших Данных»

Еще одним направлением эффективного применения технологий Больших Данных является прогноз развития социальных, политических, военных и экономических процессов. При этом к началу нулевых годов

специалисты, ведущие исследования в этой сфере, сформулировали по меньшей мере, три фундаментальных положения [58]:

- используя самые изощренные и эффективные методы, можно прогнозировать процессы, но не события;
- прогнозы с высокой степенью вероятности можно делать в отношении групп различной размерности, но не отдельных индивидуумов;
- знания о действиях групп и индивидуумов в одной ситуации не позволяет давать точные прогнозы о подобных действиях, осуществляемых в другой ситуации.

Соответственно, оказалось, что различного рода прогнозы, базирующиеся на традиционных выборках, построении сценариев, экстраполяции не обладают высоким уровнем адекватности. Развитие Интернета дало возможность оперировать Большими Данными относительно человеческого поведения, намерений, желаний и т.п. Прогнозирование на основе Больших Данных состоит в извлечении нетривиальных выводов из заранее известных характеристик, признаков и сведений об объектах. Использование Больших Данных из Интернета, как огромного, пополняемого в режиме реального времени поведенческого архива для прогнозирования развивается по трем ключевым направлениям [58]:

- прямой интеллектуальный анализ общедоступных данных, предоставляемых поисковыми системами и различного рода социальными сетями и платформами;
- создание рекомендательных систем, которые прогнозируют различного рода выбор субъектов и групп, и на этой основе рекомендуют им что угодно – от книг до кандидатов в президенты;
- создание сложных прогностических систем, использующих разнородные данные, получаемые из открытой и закрытой части глобальной сети, обрабатываемые с помощью большинства известных методов интеллектуального анализа данных.

В качестве одного из наиболее ярких примеров успешного создания средства разведки как сложной прогнозной системы можно привести проект Recorded Future. Система Recorded Future базируется на трех основных элементах [58].

1. *Поисковая система третьего поколения*, которая ищет не только объекты, соответствующие поисковым запросам, и не только связи между документами, но и взаимосвязи между объектами, их характеристиками и отношениями, содержащимися в различных документах [58].

2. *Разделение информационного поля на составляющие – события, мнения, реакции*. В Recorded Future выделено три класса сообщений. Первый – это сообщения о событиях. События – это длящиеся определенный, достаточно небольшой период времени устойчивые конфигурации, которые характеризуются единством времени, места, участников и т.п. К событиям Recorded Future относит то, что может быть интерпретировано как факты, то, что реально произошло или происходит в данный момент. Второй – это мнения. К мнениям относятся любые сообщения относительно прошлых, настоящих

или будущих событий, высказанные в авторитетных источниках, либо авторитетными людьми. Наконец, третий – это реакции. Здесь принимаются во внимание любые спонтанные реакции людей на те или иные ожидаемые события, зафиксированные в различного рода текстовых сообщениях. Такое разделение на три сегмента информационного поля, как выяснилось, позволяет достаточно хорошо улавливать как господствующие тенденции и опережающим образом реагировать на их изменения, так и выявлять слабые сигналы [58].

3. *Рассмотрение Интернета как огромной распределенной сетевой базы неструктурированных данных*. Recorded Future использует поисковик, работающий в сегментированном информационном пространстве в масштабе огромной сетевой базы данных. В сетевой базе данных разные объекты и их характеристики связаны друг с другом прямыми, обратными и опосредованными связями. Соответственно, такой подход позволяет выявлять не только явные и очевидные связи, но и вести так называемый латентный анализ, т.е. получать неочевидные, а иногда даже и абсолютно не предполагаемые связи и отношения. К тому же обрабатывать огромное количество информации в алгоритмическом режиме. Т.е. оперировать информационными массивами, непосильными для непосредственной обработки человеком [58].

В настоящее время Recorded Future используется в трех сферах: государственной разведке и безопасности, в бизнесе, и в финансах для разработки инвестиционных стратегий [58].

Другим ярким примером прогностических систем нового поколения является система Quid. Эта система создана известным американским программистом и разработчиков Ш. Горли на деньги знаменитого П. Тиля, чья разведывательная программа Palantir является давно и эффективно используемым средством американского разведывательного сообщества [58].

Таким образом, Большие Данные обеспечили появление новых, на порядки более эффективных, чем раньше, методов прогнозирования научно-технических, инженерно-технологических, инвестиционных, политических, социальных и военных процессов. Эти методы в совокупности с методиками глубокого анализа на основе все тех же Больших Данных позволяют говорить о создании принципиально нового вида информационного оружия, а именно – прогностических средств. Этот вид оружия может быть использован как обеспечивающий механизм для разработки и применения традиционных вооружений.

3.10.4 Средства манипуляции и формирования поведения социальных групп на основе технологий «Больших Данных»

Как показано выше, наличие огромного всеобъемлющего поведенческого архива позволило компаниям-владельцам Больших Данных использовать их для предсказания поведения. Вместе с тем прогнозирование поведения социальных групп в тех или иных условиях позволяет решить и другую задачу – выбора условий и воздействий, при которых бы целевая социальная группа

действовала бы необходимым, заранее предопределенным, образом. В работе [59] для такой манипуляции в отношении целевых социальных групп введено понятие «подталкивание» («nudge»).

«Подталкивание» представляет собой комплекс способов использования поведенческих стереотипов, психофизио-логических реакций и технологий Больших Данных для целенаправленной коррекции поведения тех или иных конкретных социальных групп. При этом выбор тех или иных факторов воздействия, которые обеспечивают реализацию эффекта «подталкивания», осуществляется на основе предсказательной аналитики полученной по итогам обработки Больших Данных [58].

Летом 2013 года было объявлено, что команды по использованию этой технологии создаются в большинстве министерств США, связанных с социальными вопросами. На них возложена задача «подталкивания» американцев к правильным с точки зрения правительства решениям не на основе объяснений, а путем использования поведенческих стереотипов, привычек и психофизиологических реакций. При этом американские СМИ высказали подозрение, что подобные команды создаются и в других, в том числе разведывательных ведомствах. Однако их финансирование реализуется через секретные статьи бюджета, и поэтому их существование не афишируется [58].

Профессионалы «подталкивания», развивая поведенческую политику, исходят из нескольких основных принципов.

- Для решения своих поведенческих проблем люди нуждаются во вмешательстве третьих лиц. Наилучшим кандидатом на эту роль является государство.
- Эксперты, изучая то влияние, которое в реальной жизни оказывают на благосостояние те или иные акты выбора, принимают от имени индивидов решения лучше тех, на которые индивиды способны сами.
- Любые стимулирующие схемы, которые возлагают на людей ответственность за последствия их прошлых действий, неэффективны. Вместо них необходимы схемы, которые немедленно вознаграждают или наказывают людей за будущие последствия их текущих действий – последствия, которые сами они неспособны осознать и учесть.
- С точки зрения политики то, как люди ощущают себя в обществе, важнее того, что они желают, или того, что они делают.

Ключевую роль в технологиях «подталкивания» играют Большие Данные. Именно Большие Данные позволяют, в зависимости от поставленной задачи проводить классификацию групп и ситуаций, осуществлять анализ и прогноз, а главное – искать факторы, обеспечивающие нужное поведение целевых групп в конкретных ситуациях. И, наконец, они в режиме реального времени позволяют отслеживать эффективность «подталкивания» [58].

Стоит отметить, что при наличии соответствующих Больших Данных фактически нет никаких ограничений для использования технологий «подталкивания» не только в отношении граждан собственной страны, но и населения любых государств мира. Таким образом, в настоящее время АНБ и

другие государственные структуры США разрабатывают и переходят к практическому использованию технологий управления групповым и массовым поведением в других странах мира – как в странах-союзниках, так и в странах-противниках.

При наличии соответствующих Больших Данных «подталкивание» может рассматриваться как эффективное информационно-психологическое оружие следующего поколения. Хотя, с учетом принципов и технологий, на которых построена система «подталкивания», более точным является не привычное наименование информационно-психологического оружия, а скорее отнесение этой технологии к поведенческому оружию, базирующемуся на симбиозе высокопроизводительных технических средств обработки, технологиях Больших Данных, достижениях объективной психологии и когнитивных науках [58].

Заключение

В работе предложен понятийный аппарат и представлен авторский подход к классификации информационного оружия в технической сфере. Классифицированы информационно-технические воздействия. Проведен анализ средств, способов и примеров применения для наиболее распространенных информационно-технических воздействий. Обоснованы их определения и их классификация.

Литература

1. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.

2. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.

3. Бедрицкий А. В. Информационная война: концепции и их реализация в США / Под ред. Е.М. Кожокина. – М.: РИСИ, 2008. – 187 с.

4. Новиков В. К. Информационное оружие – оружие современных и будущих войн. – М.: Горячая линия - Телеком, 2011. – 264 с.

5. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия // Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 104-146.

6. Воронцова Л. В., Фролов Д. Б. История и современность информационного противоборства. – М.: Горячая линия - Телеком, 2006. – 192 с.

7. Шеховцов Н. П., Кулешов Ю. Е. Информационное оружие: теория и практика применения в информационном противоборстве // Вестник Академии военных наук. 2012. № 1 (38). С. 35-40.

8. Паршакова Е. Д. Информационные войны: учебное пособие – Краматорск: ДГМА, 2012. – 92 с.

9. Информационная война и защита информации. Словарь основных терминов и определений. – М.: Центр стратегических оценок и прогнозов, 2011. – 68 с.

10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.

11. Прокофьев В. Ф. Тайное оружие информационной войны. Воздействие на подсознание. – М.: Синтег, 2003. – 430 с.

12. Расторгуев С. П. Информационная война. – М.: Радио и связь, 1999. – 416 с.

13. Буренок В.М., Ивлев А.А., Корчак В.Ю. Развитие военных технологий XXI века: проблемы планирование, реализация. – Тверь: Издательство ООО «КУПОЛ», 2009. – 624 с.

14. Буянов В. П., Ерофеев Е. А., Жогла Н. Л., Зайцев О. А., Курбатов Г. Л., Петренко А. И., Уфимцев Ю. С., Федотов Н. В. Информационная безопасность России – М.: Издательство «Экзамен», 2003. – 560 с.

15. Абдурахманов М. И., Баришполец В. А., Баришполец Д. В., Манилов В. Л. Геополитика, международная и национальная безопасность. Словарь основных понятий и определений / Под общей ред. В.Л. Манилова. – М.: РАЕН, 1998. – 256 с.

16. Хогг О. Эволюция оружия. От каменной дубинки до гаубицы / Пер. с англ. Л.А. Игоревского. – М.: ЗАО Центрполиграф, 2008. – 250 с.

17. Колин К. К. Социальная информатика. – М.: Академический проект, 2003. – 432 с.

18. Остапенко О. Н., Баушев С. В, Морозов И. В. Информационно-космическое обеспечение группировок войск (сил) ВС РФ: учебно-научное издание. – СПб.: Любавич, 2012. – 368 с.

19. Паршин С. А., Горбачев Ю. Е., Кожанов Ю. А. Кибервойны – реальная угроза национальной безопасности. – М.: КРАСАНД, 2011. – 96 с.

20. Проблемы безопасности программного обеспечения / Под ред. П.Д. Зегжды. – СПб.: ГТУ, 1995. – 200 с.

21. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

22. Медведовский И. Д., Семьянов П. В., Платонов В. В. Атака через Интернет / Под ред. П.Д. Зегжды. – СПб.: Изд. НПО «Мир и семья-95», 1997. – 277 с.

23. DoS-атака // Wikipedia [Электронный ресурс]. 19.05.2016. – URL: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 (дата доступа 19.05.2016).

24. Марков А. С., Фадин А. А. Организационно-технические проблемы защиты от целевых вредоносных программ // Вопросы кибербезопасности. 2013. № 1 (1). С. 28-36.

25. Duqu: A Stuxnet-like malware found in the wild, technical report. Laboratory of Cryptography of Systems Security (CrySyS). – Budapest: Budapest University of Technology and Economics Department of Telecommunications, 2011.

– 60 p. – URL: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf (дата доступа 20.08.2016).

26. Вирус Regin // Security Lab [Электронный ресурс]. 28.05.2015. – URL: http://www.securitylab.ru/analytics/473080.php (дата доступа 14.08.2016).

27. Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации: учебное пособие. – М.: Издательский центр «Академия», 2006. – 256 с.

28. Шабанов А. Программные закладки в бизнес-приложениях // Anti-Malware [Электронный ресурс]. 13.01.2011. – URL: http://www.anti-malware.ru/software_backdoors# (дата доступа 14.08.2016).

29. Дождиков В. Г., Салтан М. И. Краткий энциклопедический словарь по информационной безопасности. – М.: ИАЦ Энергия, 2010. – 240 с.

30. Зайцев О. Современные клавиатурные шпионы // Компьютер Пресс [Электронный ресурс]. 2006. № 5. – URL: http://www.compress.ru/Archive/CP/2006/5/23/ (дата доступа 14.08.2016).

31. Виноградов А. А. Функциональность, надежность, кибер-устойчивость в системах автоматизации критических инфраструктур [Доклад] // Конференция «Региональная информатика-2012». – СПб.: ОАО «НПО «Импульс», 2012.

32. Каталог АНБ США. 2014. 48 с. [Электронный ресурс]. – URL: http://s3r.ru/13/01/2014/novosti/raskryit-spisok-apparatnyih-zakladok-anb-ssha-dlya-tehniki-cisco-huawei-i-juniper-katalog/attachment/48-stranits-kataloga-abn-ssha/ (дата доступа 14.08.2016).

33. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура // Вопросы кибербезопасности. 2014. № 2 (3). С. 60-65.

34. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 2. Рабочее место оператора // Вопросы кибербезопасности. 2014. № 4 (7). С. 60-68.

35. Китайские закладки. Голый король // Security Lab [Электронный ресурс]. 30.09.2012. – URL: http://www.securitylab.ru/contest/430512.php?pagen=7&el_id=430512 (дата доступа 14.08.2016).

36. Марков А. С., Цирлов В. Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). С. 42-48.

37. Тихонов А. Ю., Аветисян А. И. Развитие taint-анализа для решения задачи поиска программных закладок // Труды Института системного программирования РАН. 2011. Т. 20. С. 9-24.

38. Гайсарян С. С., Чернов А. В., Белеванцев А. А., Маликов О. Р., Мельник Д. М., Меньшикова А. В. О некоторых задачах анализа и трансформации программ // Труды Института системного программирования РАН. 2004. Т. 5. С. 7-40.

39. Чукляев И. И. Анализ уязвимостей в исходных кодах программного обеспечения статическими и динамическими методами // XII Всероссийское совещание по проблемам управления «ВСПУ-2014», 16-19 июня 2014 г. – М., 2014. – С. 9232-9242.

40. Шурдак М. О., Лубкин И. А. Методика и программное средство защиты кода от несанкционированного анализа // Программные продукты и системы. 2012. № 4. С. 176-180.

41. Язов Ю. К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.

42. Сердечный А. Л. Инновационный подход к защите информации в виртуальных вычислительных сетях, основанный на стратегии обмана // Информация и безопасность. 2013. № 3. С. 399-403.

43. Булойчик В. М., Берикбаев В. М., Герцев А. В., Русак И. Л., Булойчик А. В., Герцев В. А., Зайцев С. И. Разработка и реализация комплекса имитационных моделей боевых действий на мультипроцессорной вычислительной системе // Наука и военная безопасность. 2009. № 4. С. 32-37. – URL: http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2009/12076-razrabotka-i-realizacija-kompleksa-imitacionnyh (дата доступа 30.07.2014).

44. Резяпов Н., Чесноков С., Инюхин С. Имитационная система моделирования боевых действий JWARS // Зарубежное военное обозрение. 2008. № 11. С. 27-32. – URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7599-imitacionnaja-sistema-modelirovanija-boevyh (дата доступа 17.08.2016).

45. Резяпов Н. Развитие систем компьютерного моделирования в вооруженных силах США // Зарубежное военное обозрение. 2007. № 6. С. 17-23. – URL: http://pentagonus.ru/publ/11-1-0-222 (дата доступа 18.08.2016).

46. Новиков Д. А. Иерархические модели военных действий // Управление большими системами: сборник трудов. 2012. № 37. С. 25-62.

47. Меньшаков Ю. К. Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

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

49. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с.

50. Емельянов С. Л. Техническая разведка и технические каналы утечки информации // Системи обробки інформації. 2010. № 3 (84). С. 20-23.

51. Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 216-223.

52. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Том 16. № 1. С. 115-118.

53. Пахомова А. С., Пахомов А. П., Юрасов В. Г. Об использовании классификации известных компьютерных атак в интересах разработки

структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 81-86.

54. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description // Cigital Inc. 2008. Vol. 3.

55. Зенин А. Разведка в сухопутных войсках США на основе анализа открытых источников информации // Зарубежное военное обозрение. 2009. № 5 С. 32-38. URL: http://pentagonus.ru/publ/80-1-0-1183 (дата доступа 17.08.2016).

56. Кондратьев А. Разведка с использованием открытых источников информации в США // Зарубежное военное обозрение. 2010. № 9. С. 28-32. URL: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/7969-razvedka-s-ispolzovaniem-otkrytyh-istochnikov (дата доступа 30.08.2016).

57. Разведка средствами Интернет // IT-сектор [Электронный ресурс]. – URL: http://it-sektor.ru/razvedka-sredstvami-internet.html (дата доступа 17.08.2016).

58. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.

59. Thaler R. H., Sunstein C. R. Nudge: Improving decisions about health, wealth, and happiness. – Yale: Yale University Press, New Haven, CT, 2008. – 293 p.

60. Кожевников Д. А., Максимов Р. В., Павловский А. В. Способ защиты вычислительной сети (варианты) // Патент на изобретение RU 2325694 C1. Опубл. 27.05.2008, бюл. № 15.

61. Гречишников Е. В., Стародубцев Ю. И., Белов А. С., Стукалов И. В., Васюков Д. Ю., Иванов И. В. Способ (варианты) управления демаскирующими признаками системы связи // Патент на изобретение RU 2450337 C1. Опубликовано 10.05.2012, Бюл. № 13.

62. Иванов В. А., Белов А. С., Гречишников Е. В., Стародубцев Ю. И., Ерышов В. Г., Алашеев В. В., Иванов И. В. Способ контроля демаскирующих признаков системы связи // Патент на изобретение RU 2419153 C2. Опубликовано: 20.05.2011, Бюл. №14.

63. Хорев А. А. Теоретические основы оценки возможностей технических средств разведки: монография. – М.: МО РФ, 2000. – 255 с.

64. Технические средства видовой разведки: учеб. пособие / Под ред. А.А. Хорева. – М.: РВСН, 1997. – 327 с.

References

1. Makarenko S. I., Chucklyaev I. I. The terminological basis of the informational conflict area. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 13-21 (in Russian).

2. Griniaev S. N. *Pole bitvy – kiberprostranstvo. Teoriia, priemy, sredstva, metody i sistemy vedeniia informatsionnoi voiny* [Battlefield – cyberspace. Theory, techniques, tools, methods and systems of information warfare]. Moscow, Kharvest Publ., 2004. 426 p. (in Russian).

3. Bedritskiy A. V. *Informatsionnaia voina: kontseptsii i ikh realizatsiia v SShA* [Information warfare: concepts and their implementation in the United States]. Moscow, The Russian Institute of Strategic Research, 2008. 187 p. (in Russian).

4. Novikov V. K. *Informatsionnoe oruzhie – oruzhie sovremennykh i budushchikh voin* [Information weapons – modern weapons and future wars]. Moscow, Goriachaia liniia - Telekom, 2011. 264 p. (in Russian).

5. Petrenko S. A. Metody informatsionno-tekhnicheskogo vozdeistviia na kibersistemy i vozmozhnye sposoby protivodeistviia [Methods information technology impact on cyber-systems and possible ways to counter]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk*, 2009, vol. 41, pp. 104-146 (in Russian).

6. Vorontsova L. V., Frolov D. B. *Istoriia i sovremennost' informatsionnogo protivoborstva* [History and modernity of information warfare]. Moscow, Goriachaia liniia - Telekom, 2006. 192 p. (in Russian).

7. Shekhovtsov N. P., Kuleshov Iu. E. Informatsionnoe oruzhie: teoriia i praktika primeneniia v informatsionnom protivoborstve [Information warfare: theory and practice in information war]. *Vestnik Akademii voennykh nauk*, 2012, vol. 38, no. 1, pp. 35-40 (in Russian).

8. Parshakova E. D. *Informatsionnye voiny: uchebnoe posobie* [The information war]. Kramatorsk, Donbass state engineering Academy, 2012. 92 p. (in Russian).

9. *Informatsionnaia voina i zashchita informatsii. Slovar' osnovnykh terminov i opredelenii* [Information warfare and information security. A Glossary of key terms and definitions]. Moscow, Center for strategic assessments and forecasts, 2011. 68 p. (in Russian).

10. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.

11. Prokofev V. F. *Tainoe oruzhie informatsionnoi voiny. Vozdeistvie na podsoznanie* [Secret weapon of the information war. Impact on the subconscious]. Moscow, Sinteg Publ., 2003. 430 p. (in Russian).

12. Rastorguev S. P. *Informatsionnaia voina* [Information war]. Moscow Radio i Sviaz Publ., 1999. 416 p. (in Russian).

13. Burenok V. M., Ivlev A. A., Korchak V. Ju. *Razvitie voennykh tekhnologii XXI veka: problemy planirovanie, realizatsiia* [The progress of military technology of the XXI century: problems of planning, implementation]. Tver, KUPOL Publ., 2009. 624 p. (in Russian).

14. Buianov V. P., Erofeev E. A., Zhogla N. L., Zaitsev O. A., Kurbatov G. L., Petrenko A. I., Ufimtsev Iu. S., Fedotov N. V. *Informatsionnaia bezopasnost' Rossii* [Russia's information security] Moscow, Ekzamen Publ., 2003. 560 p. (in Russian).

15. Abdurakhmanov M. I., Barishpolets V. A., Barishpolets D. V., Manilov V. L. *Geopolitika, mezhdunarodnaia i natsional'naia bezopasnost'. Slovar' osnovnykh poniatii i opredelenii* [Geopolitics, international and national security. A dictionary of basic concepts and definitions]. Moscow, Russian Academy of natural Sciences, 1998. 256 p. (in Russian).

16. Khogg O. *Evoliutsiia oruzhiia. Ot kamennoi dubinki do gaubitsy* [The evolution of arms. From stone club to howitzers]. Moscow, Tsentrpoligraf Publ., 2008. 250 p. (in Russian).

17. Kolin K. K. *Sotsial'naia informatika* [Social Informatics]. Moscow, Akademicheskii proekt Publ., 2003. 432 p. (in Russian).

18. Ostapenko O. N., Baushev S. V, Morozov I. V. *Informatsionno-kosmicheskoe obespechenie gruppirovok voisk (sil) VS RF: uchebno-nauchnoe izdanie* [Information and space security groups of troops (forces) of the armed forces]. Saint-Peterburg, Liubavich Publ., 2012. 368 p. (in Russian).

19. Parshin S. A., Gorbachev Iu. E., Kozhanov Iu. A. *Kibervoiny – real'naia ugroza natsional'noi bezopasnosti* [Cyberwarfare is a real threat to national security]. Moscow, KRASAND Publ., 2011. 96 p. (in Russian).

20. Zegzhdy P. D. Problemy bezopasnosti programmnogo obespecheniia [Security issues software]. Saint-Peterburg, St. Petersburg state Polytechnical University named after Peter the Great, 1995. 200 p. (in Russian).

21. Makarenko S. I. *Information security*. Stavropol, Sholokhov Moscow State University for the Humanities (Stavropol Branch) Publ., 2009, 372 p. (in Russian).

22. Medvedovskii I. D., Semianov P. V., Platonov V. V. *Ataka cherez Internet* [Attack online]. Saitn-Petersburg, "Mir i semia-95" Publ., 1997. 277 p. (in Russian).

23. Denial-of-service attack. *Wikipedia*, 19 May 2016. Available at: https://en.wikipedia.org/wiki/Denial-of-service_attack (accessed 19 May 2016).

24. Markov A. S., Fadin A. A. Organizational and technical problems of protection againsttargeted malware such as Stuxnet. *Voprosy kiberbezopasnosti*, 2013, vol. 1, no. 1, pp. 28-36 (in Russian).

25. Duqu: A *Stuxnet-like malware found in the wild, technical report. Laboratory of Cryptography of Systems Security (CrySyS)*. Budapest, Budapest University of Technology and Economics Department of Telecommunications, 2011. 60 p. Available at: http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf (accessed 20 August 2016).

26. Regin Virus. *Security Lab*, 28 May 2015. Available at: http://www.securitylab.ru/analytics/473080.php (accessed 14 August 2016) (in Russian).

27. Kuprijanov A. I., Saharov A. V. Shevtsov V. A. *Osnovy zashchity informatsii* [The basics of information security]. Moscow, Publishing center «Akademia», 2006. 256 p. (in Russian).

28. Shabanov A. Programmnye zakladki v biznes-prilozheniiakh [Backdoors in business applications]. *Anti-Malware*, 13 January 2011. Available at: http://www.anti-malware.ru/software_backdoors# (accessed 14 August 2016) (in Russian).

29. Dozhdikov V. G., Saltan M. I. *Kratkii entsiklopedicheskii slovar' po informatsionnoi bezopasnosti* [Short encyclopedic dictionary of information security]. Moscow, Energiia Publ., 2010. 240 p. (in Russian).

30. Zaitsev O. Sovremennye klaviaturnye shpiony [Modern keyloggers]. *Computer Press*, 2006, no. 5. Available at:

http://www.compress.ru/Archive/CP/2006/5/23/ (accessed 14 August 2016) (in Russian).

31. Vinogradov A. A. Funktsional'nost', nadezhnost', kiber-ustoichivost' v sistemakh avtomatizatsii kriticheskikh infrastruktur [Functionality, reliability, cyber-resilience in the automation systems of critical infrastructures]. *Konferentsiia "Regional'naia informatika-2012"* [Proceedings of Conference "Regional Informatics-2012"]. Saint-Petersburg, "Impul's" Scientific Production Association, 2012.

32. Catalog of the NSA. 2014. 48 p. Available at: http://s3r.ru/13/01/2014/novosti/raskryit-spisok-apparatnyih-zakladok-anb-ssha-dlya-tehniki-cisco-huawei-i-juniper-katalog/attachment/48-stranits-kataloga-abn-ssha/ (accessed 14 August 2016).

33. Klyanchin A. I. The NSA's spy catalog. Part 1. Infrastructure. *Voprosy kiberbezopasnosti*, 2014, vol. 3, no. 2, pp. 60-65 (in Russian).

34. Klyanchin A. I. The NSA's spy catalog. Part 2. Operator's workplace. *Voprosy kiberbezopasnosti*, 2014, vol. 7, no. 4, pp. 60-68 (in Russian).

35. Kitaiskie zakladki. Golyi korol [Chinese bookmarks. The naked king]. *Security Lab*. 30 September 2012. Available at: http://www.securitylab.ru/contest/430512.php?pagen=7&el_id=430512 (accessed 14 August 2016) (in Russian).

36. Markov A. S., Tsirlov V. L. Experience in identifying vulnerabilities in software. *Voprosy kiberbezopasnosti*, 2013, vol. 1, no. 1, pp. 42-48 (in Russian).

37. Tikhonov A. Iu., Avetisian A. I. Razvitie taint-analiza dlia resheniia zadachi poiska programmnykh zakladok [Development of taint-analysis for solving the problem of finding software bugs]. *Proceedings of the Institute for System Programming of the RAS*, 2011, vol. 20, pp. 9-24 (in Russian).

38. Gaisarian S. S., Chernov A. V., Belevantsev A. A., Malikov O. R., Melnik D. M., Menshikova A. V. O nekotorykh zadachakh analiza i transformatsii program [On some problems of the analysis and transformation of programs]. *Proceedings of the Institute for System Programming of the RAS*, 2004, vol. 5, pp. 7-40 (in Russian).

39. Chukliaev I. I. Analiz uiazvimostei v iskhodnykh kodakh programmnogo obespecheniia staticheskimi i dinamicheskimi metodami [The analysis of vulnerabilities in source code of the software static and dynamic methods]. *XII Vserossiiskoe soveshchanie po problemam upravleniia "VSPU-2014"* [XII all-Russia meeting on control problems, "VCPU-2014"], Moscow, 2014. pp. 9232-9242 (in Russian).

40. Shurdak M. O., Lubkin I. A. Metodika i programmnoe sredstvo zashchity koda ot nesanktsionirovannogo analiza [The methodology and software tool code protection against unauthorized analysis]. *Programmnye produkty i sistemy*, 2012, no. 4, pp. 176-180 (in Russian).

41. Yazov Yu. K., Serdechnyy A. L., Sharov I. A. Methodical approach for estimation of efficiency of honeypot system. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 55-60 (in Russian).

42. Serdechnyy A. L. The innovation approach, based on strategy of deception, to information security of virtual networks. *Informatsiia i bezopasnost*, 2013, no. 3, pp. 399-403 (in Russian).

43. Buloichik V. M., Berikbaev V. M., Gertsev A. V., Rusak I. L., Buloichik A. V., Gertsev V. A., Zaitsev S. I. Razrabotka i realizatsiia kompleksa imitatsionnykh modelei boevykh deistvii na mul'tiprotsessornoi vychislitel'noi sisteme [Development and implementation of a complex simulation models fighting in a multiprocessor computing system]. *Nauka i voennaia bezopasnost*, 2009, no. 4, pp. 32-37. Available at: http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2009/12076-razrabotka-i-realizacija-kompleksa-imitacionnyh (accessed 30 July 2016) (in Russian).

44. Reziapov N., Chesnokov S., Iniukhin S. Imitatsionnaia sistema modelirovaniia boevykh deistvii JWARS [Simulation the simulation system of hostilities JWARS]. *Zarubezhnoe voennoe obozrenie*, 2008, no. 11, pp. 27-32. Available at: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2008-zvo/7599-imitacionnaja-sistema-modelirovanija-boevyh (accessed 17 August 2016) (in Russian).

45. Reziapov N. Razvitie sistem komp'iuternogo modelirovaniia v vooruzhennykh silakh SShA [Development of systems for computer modeling in the U.S. armed forces]. *Zarubezhnoe voennoe obozrenie*, 2007, no. 6, pp. 17-23. Available at: http://pentagonus.ru/publ/11-1-0-222 (accessed 18 August 2016) (in Russian).

46. Novikov D. A. Hierarchical models of combat. *Upravlenie bol'simi sistemami*, 2012, no. 37, pp. 25-62 (in Russian).

47. Menshakov Iu. K. *Teoreticheskie osnovy tekhnicheskikh razvedok* [The theoretical basis of technical intelligence]. Moscow, Bauman Moscow State Technical University Publ., 2008. 536 p. (in Russian).

48. Chukliaev I. I., Morozov A. V., Bolotin I. B. *Teoreticheskie osnovy optimal'nogo postroeniia adaptivnykh sistem kompleksnoi zashchity informatsionnykh resursov raspredelennykh vychislitel'nykh sistem: monografiia* [Theoretical Foundations of Optimal Construction of Adaptive Systems of Comprehensive Protection of Information Resources Distributed Computing Systems. Monograph] Smolensk, Military Academy of Army Air Defence Publ., 2011. 227 p. (in Russian).

49. Khoroshko V. A., Chekatkov A. A. *Metody i sredstva zashchity informatsii* [Methods and means of information protection]. Kiev, Iunior Publ., 2003. 504 p. (in Russian).

50. Emelianov S. L. Tekhnicheskaia razvedka i tekhnicheskie kanaly utechki informatsii [Technical intelligence technical channels of information leakage]. *Sistemi obrobki informatsiï*, 2010, vol. 84, no. 3, pp. 20-23 (in Russian).

51. Varlamov O. O. O sistemnom podkhode k sozdaniiu modeli komp'iuternykh ugroz i ee roli v obespechenii bezopasnosti informatsii v kliuchevykh sistemakh informatsionnoi infrastruktury [A systematic approach to creating models of computer threats and its role in information security in the key systems of

information infrastructure]. *Izvestiya SFedU. Engineering sciences*, 2006, vol. 62, no. 7, pp. 216-223 (in Russian).

52. Pakhomova A. S., Pakhomov A. P., Razinkin K. A. To the problem of the development of a structural model of computer intelligence. *Informatsiia i bezopasnost*, 2013, vol. 16, no. 1, pp. 115-118 (in Russian).

53. Pakhomova A. S., Pakhomov A. P., Yurasov V. G. To the implementation of the known computer attacks classification to develop a structural model of computer intelligence. *Informatsiia i bezopasnost*, 2013, vol. 16, no. 1, pp. 81-86 (in Russian).

54. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description. *Cigital Inc*, 2008, Vol. 3.

55. Zenin A. Razvedka v sukhoputnykh voiskakh SShA na osnove analiza otkrytykh istochnikov informatsii [Intelligence in the United States army based on the analysis of open source information]. *Zarubezhnoe voennoe obozrenie*, 2009, no. 5, pp. 32-38. Available at: http://pentagonus.ru/publ/80-1-0-1183 (accessed 17 August 2016) (in Russian).

56. Kondratev A. Razvedka s ispol'zovaniem otkrytykh istochnikov informatsii v SShA [Intelligence using open sources of information in the United States]. *Zarubezhnoe voennoe obozrenie*, 2010, no. 9, pp. 28-32. Available at: http://militaryarticle.ru/zarubezhnoe-voennoe-obozrenie/2010-zvo/7969-razvedka-s-ispolzovaniem-otkrytyh-istochnikov (accessed 30 August 2016) (in Russian).

57. Razvedka sredstvami Internet [The exploration of Internet tools]. *IT-sector*, 2016. Available at: http://it-sektor.ru/razvedka-sredstvami-internet.html (accessed 17 August 2016) (in Russian).

58. Larina E. S., Ovchinskii V. S. *Kibervoiny XXI veka. O chem umolchal Edvard Snouden* [Cyberwar XXI century. What silent Edward Snowden]. Moscow, Knizhnyi Mir Publ., 2014. 352 p. (in Russian).

59. Thaler R. H., Sunstein C. R. *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press, New Haven, CT, 2008. 293 p.

60. Kozhevnikov D. A., Maksimov R. V., Pavlovskii A. V. Sposob zashchity vychislitel'noi seti (varianty) [Method of protecting computer network (variants)]. Patent Russia, no. RU 2325694 C1. Publish. 27.05.2008, bul. no. 15 (in Russian).

61. Grechishnikov E. V., Starodubtsev Iu. I., Belov A. S., Stukalov I. V., Vasiukov D. Iu., Ivanov I. V. Sposob (varianty) upravleniia demaskiruiushchimi priznakami sistemy sviazi [Method (variants) control telltale signs of a communication system]. Patent Russia, no. RU 2450337 C1. Publish. 10.05.2012, bul. no. 13 (in Russian).

62. Ivanov V. A., Belov A. S., Grechishnikov E. V., Starodubtsev Iu. I., Eryshov V. G., Alasheev V. V., Ivanov I. V. Sposob kontrolia demaskiruiushchikh priznakov sistemy sviazi [Method of control of the telltale signs of a communication system]. Patent Russia, no. RU 2419153 C2. Publish. 20.05.2011, bul. no. 14 (in Russian).

63. Khorev A. A. *Teoreticheskie osnovy otsenki vozmozhnostei tekhnicheskikh sredstv razvedki: monografiia* [The theoretical basis for the estimation of

opportunities of technical means of intelligence. Monograph]. Moscow, The Ministry of Defence, 2000. 255 p. (in Russian).

64. Khorev A. A. *Tekhnicheskie sredstva vidovoi razvedki* [Technical means imagery intelligence]. Moscow, Strategic Rocket Forces Publ., 1997. 327 p. (in Russian).

Статья поступила 26 сентября 2016 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.

Information Weapon in Technical Area – Terminology, Classification and Examples

S. I. Makarenko

Relevance. *For review of information warfare is necessary forming the terminological basis. An information weapon is main term of the terminological basis of information warfare. Theory of information weapon in psychological warfare is widely researched at well-known papers. However, theory of information weapon in technical area has not widely researched. Therefore, forming terminological basis for the information weapon in technical area and its classification is topical.* ***The aim of this paper*** *is forming the terminological basis and the classification systems for the information weapon in technical area.* ***Novelty.*** *The element of novelty of this paper is forming the new terms and the new classification systems for the review of information weapon in technical area by author's way. Also novelty items are trends of improvement of some types of information weapon which detect by author.* ***Practical relevance.*** *The review presented can be used by technical specialists to make a new technology in the areas of the information warfare and the information security. Also this review can be used military specialists for elaborating new forms and methods of armed struggle with use of an information weapon.*

Key words: *information struggle, information weapon, information warfare, information attack, network attack, virus, software beetle, hardware beetle, neutralizer for tests software, mock object of information area, software for modeling of combat acts, radio reconnaissance, open source Intelligence, Big Date.*

Information about Author

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Associate Professor at the Department of Networks and Communication Systems of Space Systems. A. F. 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, Zjdanovskaya ulica, 13.