Научно-технических журнал

ТЕХНИКА СРЕДСТВ СВЯЗИ

MEANS OF COMMUNICATION EQUIPMENT

Scientific and Technical Journal

№ 3 (151) – 2020

РЕДАКЦИЯ: Верстка принт-макета: **Мамончикова А.С.**
Дизайн обложки: **Шаутин Д.В.**
Поддержка сетевой версии журнала: **Лебедев Д.А.**
Секретарь редакции: **Михайлова Н.В.**

АДРЕС РЕДАКЦИИ: 197342. Россия. г. Санкт-Петербург, ул. Кантемировская, дом 8,
Телефон: +7(812) 542-90-54; +7(812) 448-95-97; +7(812) 448-96-84
Факс: +7(812) 542-18-49. E-mail: intelteh@inteltech.ru.
Официальный сайт: www.inteltech.ru; www.mce-journal.ru

Научно-технических журнал
ТЕХНИКА СРЕДСТВ СВЯЗИ
MEANS OF COMMUNICATION EQUIPMENT
Scientific and Technical Journal
№ 3 (151) – 2020

Научно-технический журнал «Техника средств связи» – это рецензируемое научное издание, в котором публикуются результаты научных исследований специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств связи и информационной безопасности. Журнал является правопреемником издававшихся с 1959 года Министерством промышленности средств связи СССР всесоюзных журналов «Вопросы радиоэлектроники. Серия: Техника проводной связи» и «Вопросы специальной радиоэлектроники. Серия: Техника проводной связи». С 1975 года журнал издается под названием «Техника средств связи». Учредитель и издатель журнала: Публичное акционерное общество «Информационные телекоммуникационные технологии» (ПАО «Интелтех»). Адрес учредителя и издателя журнала: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

СОДЕРЖАНИЕ

CONTENTS

Рубрики журнала: Анализ новых технологий и перспектив развития техники средств связи • Системы управления • • Передача, прием и обработка сигналов • Системы связи и телекоммуникации • Перспективные исследования • • Вычислительные системы • Информационные процессы и технологии. Сбор, хранение и обработка информации • • Моделирование сложных организационно-технических систем • Вопросы обеспечения информационной безопасности • • Интеллектуальные информационные системы • Робототехнические системы • Электронные и радиотехнические системы • • Объекты интеллектуальной собственности и инновационные технологии в области разработки средств телекоммуникаций

СИСТЕМЫ СВЯЗИ И ТЕЛЕКОММУНИКАЦИИ

УДК 621.396.24: 621.371.38

Использование частотного ресурса системой декаметровой связи в режиме псевдослучайной перестройки рабочей частоты

Панин Р.С., Путилин А.Н., Хвостунов Ю.С.

Аннотация. *В статье рассматривается постановка задачи совместной оптимизации выбора рабочих частот и параметров алгоритма множественного доступа для сети декаметровой связи. Исследуется режим псевдослучайной перестройки рабочей частоты с частотно-временным разделением радиоканалов различных абонентов. В системах радиосвязи с псевдослучайной перестройкой рабочей частоты отсутствует традиционно использовавшееся закрепление рабочих частот за радиолиниями, что делает существующие методы назначения рабочих частот не эффективными. Целью работы является постановка задачи совместной оптимизации выбора рабочих частот и параметров алгоритма множественного доступа в сети декаметровой радиосвязи. Используются теоретический и практический заделы в области цифровой передачи данных по декаметровому каналу связи. Новизна работы состоит в формулировке задачи совместной оптимизации выбора рабочих частот и параметров алгоритмов множественного доступа. Практический результат работы определяет появляющаяся возможность автоматизации процесса подготовки радиоданных в автоматизированной системе управления связи. Также групповое использование частот обеспечивает существенный прирост эффективности функционирования сети декаметровой радиосвязи.*

Ключевые слова*: декаметровая радиосвязь; псевдослучайная перестройка рабочей частоты; частотный ресурс; алгоритм множественного доступа***.**

Введение

Сети дальней радиосвязи используются критическими инфраструктурами управления как аварийные в чрезвычайных ситуациях, когда основная сеть связи выходит из строя, вследствие природной катастрофы или военного конфликта. Наибольшие возможности для этого предоставляет декаметровая радиосвязь, поскольку она обеспечивает информационный обмен с высокими скоростями на большие расстояния. Однако, готовность и надёжность сетей декаметровой радиосвязи, в настоящее время, не соответствуют предъявляемым требованиям.

Причина заключается в низком уровне автоматизации установления, поддержания, восстановления и разрыва сеансов радиосвязи в автоматизированных системах управления связью (АСУС). Имеет место фиксированное закрепление рабочих частот, определяемых радиоданными, за радиоканалами при их организации.

Под радиоканалом в рамках данной работы, в соответствии с Рекомендацией *ITU-R F*.1487 [1] будем понимать комплекты передающих и приёмных радиосредств с выхода модулятора до входа демодулятора, функционирующие в заранее определенном рабочем режиме, который характеризуется шириной спектра формируемого сигнала, видом и кратностью модуляции, используемым канальным кодированием, последовательностью использования закрепленных рабочих частот.

Радиоканал может использоваться для организации радионаправления или радиосети. В настоящее время, при неудовлетворительном качестве прохождения радиосигнала, нужна коррекция рабочих частот со стороны должностных лиц АСУС. Поэтому необходим переход от ручного и автоматизированного установления и поддержания соединений к автоматическому, при свободном использовании всех разрешенных рабочих частот радиостанциями, в режиме множественного доступа.

В качестве частного примера реализации такого подхода можно привести самоорганизующиеся сети радиосвязи (ССР). Это радиосети с децентрализованным

управлением, не имеющие постоянной структуры. При наличии доступности, любые радиостанции могут соединяться в произвольном порядке. Частотный ресурс используется коллективно. Каждая абонентская радиостанция может быть ретранслятором, динамически определяя направления пересылки чужих данных. ССР не разделяются на подсети абонентского доступа и магистральные транспортные каналы между станциями доступа, что имеет место для большинства существующих в РФ сетей дальней радиосвязи. Как правило, данные сети строятся на технологии коммутации пакетов, и развертываются для обслуживания мобильных абонентов.

В англоязычной литературе для их обозначения часто используется термин «мобильная сеть с ситуационным управлением», *Mobile Ad hoc Network* (*MANET*). Они обеспечивают возможность передачи данных на большие расстояния без увеличения мощности передатчика, устойчивость к изменениям в инфраструктуре сети, простоту и высокую скорость развертывания. Существующие реализации ССР основаны на технологиях *Bluetooth, Wi-Fi, ZigBee*, не использующих декаметровый диапазон. Перспективная военная радиосистема связи армии США *Joint Tactical Radio System* (*JTRS*) использует закрытый сетевой протокол радиосвязи *Wideband Networking Waveform* (*WNW*), обеспечивающий возможность создания ССР на радиосредствах декаметрового диапазона. Отечественные протоколы функционирования ССР декаметрового диапазона и их реализации, на настоящее время, отсутствуют.

В декаметровом диапазоне на пути использования частотного ресурса сети в режиме множественного доступа возникает ключевая проблема. Это анизотропия радиоканалов декаметрового диапазона как по направлению передачи, так и по рабочей частоте. Она обусловлена тем, что вследствие использования отражения радиоволн от ионосферы, одни и те же рабочие частоты обеспечивают различные уровни сигнала на приёме в разных направлениях связи. Рабочая частота, пригодная для обмена данными в одном направлении, может быть совершенно непригодной для обмена в другом направлении. В приведенных выше примерах ССР имеет место преимущественная изотропия, то есть любая рабочая частота на любом направлении передачи имеет, примерно, одинаковое качество. Анизотропия рабочих частот и направлений передачи приводит к невозможности использования радиостанциями сети свободных рабочих частот в произвольном порядке. Данный выбор должен быть обусловлен состоянием ионосферы, взаимным положением корреспондирующих радиостанций, а также характеристиками их радиосредств.

Острота данной проблемы снижается при использовании всеми станциями сети сигналов с последовательным расширением спектра, то есть систем радиосвязи с псевдослучайной перестройкой рабочей частоты (ППРЧ). Эти системы используют для установления соединения не одну частоту, а группу стартовых рабочих частот. После установления соединения по каналу обратной связи передаются служебные данные для автоматической замены непригодных стартовых рабочих частот на запасные рабочие частоты. Вероятность наличия для любого направления связи хотя бы одной пригодной рабочей частоты растет с увеличением числа стартовых частот. С другой стороны, увеличение этого числа выше потребностей радиосети, определяемых входной нагрузкой, приводит к нерациональному использованию частотного ресурса, вследствие простоя радиоканалов. В работах [4-6] приведено описание технологии функционирования защищенной пакетной сети декаметровой радиосвязи с ППРЧ.

Выбор группы рабочих частот (ГРЧ) для установления и поддержания соединения в сети режима ППРЧ и алгоритм множественного доступа (АМД), определяющий порядок их использования радиостанцией, непосредственно связаны и взаимно зависимы. Для различных подсетей и направлений связи рабочие частоты и АМД могут различаться.

Так, например, в ближней и дальней зонах будут оптимальны ГРЧ различных поддиапазонов. Оптимальная вероятность захвата АМД канала доступа или «настойчивость протокола» будет зависеть от количества частот в группе.

При данном выборе должны быть учтены следующие факторы:

- пригодность каждой рабочей частоты для установления соединения в различных направлениях радиосвязи и радиосетях, образуемых в соответствии со схемой организации связи (СхОС);
- доля нагрузки, передаваемой в данном направлении или подсети.

Последовательность решения задачи нахождения оптимальных ГРЧ и АМД:

- математическое описание параметров, определяющих свойства среды распространения для сети;
- математическое описание параметров, определяющих порядок функционирования радиостанций как элементов сети;
- математическое описание параметров, описывающих возникновение нагрузки в сети;
- математическое описание параметров, описывающих рассматриваемый класс АМД;
- предложения по оценке эффективности функционирования сети;
- формулировка задачи оптимизации рассматриваемых АМД;
- разработка методики оптимизации данных алгоритмов;
- разработка предложений по подбору оптимальных ГРЧ и АМД.

В работе предлагается к рассмотрению формализованная постановка данной задачи.

1 Технология передачи данных в декаметровом диапазоне в режиме ППРЧ

В данном разделе приведены только ключевые моменты технологии передачи данных в декаметровом диапазоне в режиме ППРЧ, существенные для представленной работы. Подробное изложение построения представленной технологии приведено в работах [4-6].

1.1 Разделение каналов

Разделение каналов многих пользователей на едином пакете частот в режиме защиты от преднамеренных помех путем псевдослучайного переключения рабочих частот (ППРЧ) происходит следующим образом:

- в радиостанциях сети реализуется единое время;
- двоичные датчики случайных чисел (ДСЧ) запускаются синхронно во всех радиостанциях;
- изменение состояния ДСЧ происходит синхронно с окончанием слота – времени, выделяемого на передачу одного пакета данных;
- из перечня разрешённых частот выбирается упорядоченное подмножество из 2^K рабочих частот, использующихся для установления соединения, а остальные частоты становятся запасными;
- текущее содержимое K последних бит ДСЧ – R принимает значения от 0 до K-1 и определяет циклический сдвиг рабочей частоты нулевого канала;
- текущая частота рабочего канала с номером L определяется как $|R + L|_K$.

Для предотвращения наложения во времени пакетов (слотов) радиостанций, удаленных от приёмника на различное расстояние, разделяются частоты четных и нечетных слотов. Это сокращает в два раза количество рабочих каналов.

При введении в слоте защитных интервалов, исключающих наложение пакетов различных станций, количество рабочих каналов равно количеству рабочих частот, что удваивает потенциальную производительность сети. Так защитный интервал в 10 мс обеспечивает отсутствие наложений пакетов радиостанций в радиусе 3000 км, что приблизительно соответствует предельной дальности односкачковых трасс. Введение защитных интервалов снижает скорость передачи на коэффициент, равный отношению длины защитного интервала к длине слота.

На рис. 1 приведен трехмерный спектр, поясняющий псевдослучайное частотно-временное разделение сигналов двух пар радиостанций. По оси *Y* расположены спектры сигнала в канале тональной частоты (КТЧ) на частотах от 0 до 15. Можно видеть различные уровни шума на различных частотах. По оси *X* – временные слоты. Длительность одного слота – 50 мс. Число рабочих частот равно 8, то есть *K* = 3. Заняты два различных канала, поэтому столкновения посылок не происходит.

1.2 Режимы установления соединения

Режимы установления соединения определяют порядок использования выделенного радиоканала: симплекс, полудуплекс и дуплекс. В первом режиме происходит вещание одной радиостанции, всем прослушивающим канал. Во втором режиме происходит переключение направления передачи в канале между корреспондирующими радиостанциями по заранее оговорённому таймауту или приёму в потоке данных специального символа, называемого «тангента». В третьем режиме происходит одновременная передача данных между двумя радиостанциями в двух разных каналах на одном пакете частот.

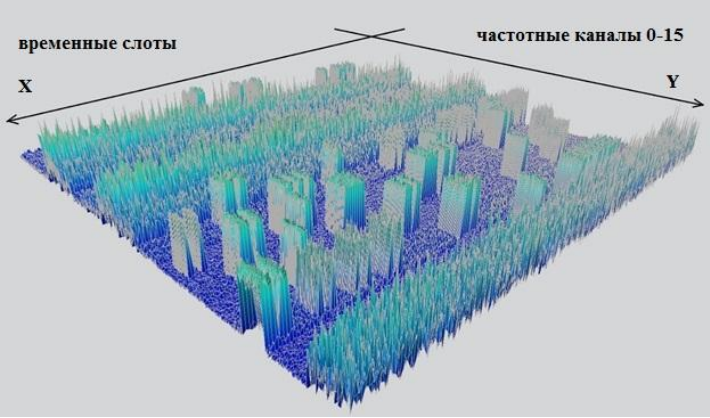


Рис. 1. Трехмерный спектр сигналов двух радиостанций

Быстрое переключение направления передачи в режиме полудуплекс может эмулировать для пользователя установление соединения в режиме дуплекс с вдвое меньшей скоростью. Это обеспечивается за счет временного разделения направления передачи в радиолинии – *Time Division Duplex* (*TDD*).

1.3 Установление соединения в режиме радио-АТС

Установление соединения в режиме радио-АТС происходит следующим образом. Приёмники станций синхронно переключаются по рабочим частотам вызывного канала с номером «0», который используется для установления соединений. При занятии чужой корреспондирующей парой нулевого канала приёмники сканируют рабочие каналы для определения их свободы или занятости. При возникновении потребности в установлении соединения вызывающая станция дожидается освобождения нулевого канала, затем вызывает корреспондента, повторяя вызов на различных частотах, и переключает направление передачи. После получения ответа корреспонденты уходят с нулевого канала на свободный канал с наименьшим номером. При занятости всех каналов, сеанс связи продолжается на нулевом канале до освобождения одного из занятых.

1.4 Адаптация по рабочим режимам

Адаптация по рабочим режимам подразумевает изменение кратности модуляции, ширины полосы, скорости корректирующего кода, мощности передачи или по части названных параметров. В процессе функционирования радиолинии приёмником измеряются:

- дисперсия разброса точек сигнального созвездия на фазовой плоскости *IQ*, по которой происходит оценка текущего отношения сигнал/помеха (*SNR, signal/noise ratio*);
- дисперсия оценок сдвигов несущей частоты, определяющая стабильность частотной синхронизации;

- дисперсия оценок сдвигов начала слота, определяющая стабильность временной синхронизации.

Все рабочие режимы упорядочиваются по возрастанию скорости в соответствии с требованиями к значениям указанных параметров. Если текущая оценка параметров позволяет увеличить скорость, то приёмник формирует передатчику корреспондирующего абонента команду на изменение рабочего режима.

1.5 Адаптация по рабочим частотам при установлении соединения

Адаптация по рабочим частотам при установлении соединения происходит следующим образом. Передаваемые в пакете данные закрываются корректирующим кодом. На приёме определяется число исправленных в слоте ошибок для каждой частоты отдельно. Если оно приближается к максимальному значению, то принимается решение на замену данной частоты. Резервная частота выбирается из запасных частот.

Процесс адаптации по рабочим частотам поясняет рис. 2. По оси абсцисс обозначены используемые часты f_0,…, f_{15}. По оси ординат – номера временных слотов. Поскольку K=3, то количество стартовых рабочих частот – 8. Режим установления соединения – полудуплекс. Первая пара установила соединение и перешла в режим частотной адаптации, в процессе которой частоты f_0 – f_3 и f_7 заменены на f_8, f_{11}, f_{12}, f_{14}, f_{15}. Произошел переход соединения на первый канал. Вторая пара находится в режиме установления соединения на нулевом канале, поэтому она использует только стартовые (начальные) частоты f_0 – f_7. Совместно всеми радиостанциями используются частоты f_4 – f_6. За счет использования корреспондирующими парами различных каналов наложения посылок не происходит.

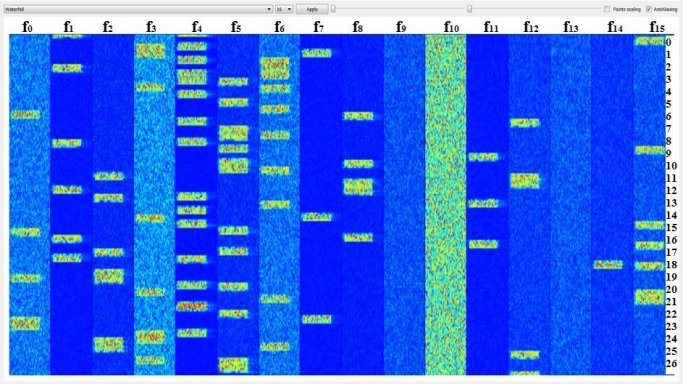


Рис. 2. Сонограмма псевдослучайного частотно-временного разделения сигналов двух корреспондирующих пар в процессе частотной адаптации и установления соединения

1.6 Перечень требуемых радиоданных

В соответствии с изложенными выше в описательной форме алгоритмами, для организации функционирования описываемой сети радиосвязи необходимо, в соответствии с единым замыслом, во все радиостанции ввести для каждого направления следующие данные:

- упорядоченный перечень стартовых и запасных частот с указанием количества стартовых частот, находящихся в начале перечня;
- ключ псевдослучайного переключения рабочих частот;
- ключ формирования имитостойкой вставки;
- перечень разрешенных рабочих режимов, определяющий полосы, кратности модуляции и режимы канального кодирования.

В рамках настоящей работы к радиоданным будем относить первый массив в указанном перечне.

Необходимо обеспечить функционирование сетевой системы единого времени, обеспечивающей во всех условиях функционирования для радиостанций сети точность определения текущего времени не хуже ± 1-3 мс.

2 Формализованное описание сети декаметровой радиосвязи и среды распространения

Для формулировки задачи необходимо формализованное описание исследуемой системы радиосвязи.

2.1 Структура сети

Структура рассматриваемой сети пакетной декаметровой радиосвязи определяется следующими параметрами. В сети имеется S радиоцентров. В соответствии с СхОС, в сети D_d – направления передачи данных.

Время занятия передатчиком рабочей частоты называется слотом: $T_s \in \{T_p; T_p + t_d\}$, где T_p – время передачи пакета или длительность посылки, t_d = const (от 2 до 100 мс) – длительность защитного интервала. Защитный интервал необходим для переключения передатчика на следующую частоту, а также он обеспечивает исключение наложения посылок разноудаленных радиостанций в соседних слотах на одной частоте. Будем полагать время дискретным по слотам передачи. Если защитный интервал меньше времени распространения сигнала на односкачковых трассах, то наложение посылок обеспечивается разделением используемых частот на две группы: для четных и нечётных слотов. Поэтому, количество одновременно устанавливаемых на пакете из F_k частот равно $N_k = F_k/2$. В противном случае, $N_k = F_k$. В зависимости от режима работы, определяемого шириной полосы низкочастотного (НЧ) сигнала, кратности модуляции и кода, на слоте может передаваться $L \in \{L_1, \ldots, L_V\}$ бит. Скорость передачи в одном радиоканале в пакетах $R = 1 / T_s$, в битах $V = L / T_s$.

Коэффициент связности сети $C = 2D_d /(S(S - 1))$, $0 \le C \le 1$, где $S(S - 1)/2$ – количество каналов в полносвязной сети. Таким образом, множество параметров, описывающих структуру сети, определяется как $\alpha = (S, D_d, T_s, L_p)$.

2.2 Среда передачи

Среда передачи в сети декаметровой радиосвязи описывается следующими параметрами. В сети разрешено использование F_S – комплекта из F_c частот [4-6], находящихся в разных участках декаметрового диапазона. Ионосферно-волновой и частотно-диспетчерской службой (ИВ ЧДС) при организации функционирования сети, априорно определена матрица вероятностей установления соединения в направлении передачи данных d на частоте f при скорости V:

$$P\,(d, f, V),$$

где $d \in \{1, \ldots, D_d\}$, $f \in \{1, \ldots, F_c\}$, а V определено выше. Эти данные могут быть получены путем экспертных оценок, из модели *IRI*-2012, зондированием рабочих частот, использованием методов зондирования ионосферы, на основе статистики прохождения радиоволн от спутников систем ГЛОНАС, *GSM*, Галилео и *BeeDo*, прослушиванием сигналов маркерных станций и станций точного времени, а также другими методами. Динамика изменения матрицы $P\,(d, f, V)$ во времени в работе не рассматривается ввиду существования периодов стационарности состояния матрицы P, на основе которых решается рассматриваемая задача оптимизации. В соответствии с числом таких периодов, в течение суток, можно подготовить соответствующее число массивов радиоданных. Следует отметить, что описание среды распространения ориентировано на использование в сети определенных типов радиосредств и модемов, поскольку только знание их характеристик позволяет определить значения вероятности для конкретной скорости передачи. Воздействие преднамеренных или системных помех на радиосеть предлагается описать количеством непригодных для каждого направления передачи частот – $F_j\,(d)$ [2]. Таким образом, среда передачи описывается множеством параметров $\delta = (P\,(d, f, V), F_j\,(d))$.

Пример: рассмотрим сеть из пяти радиоцентров с классической топологией «домик на боку», приведенной на рис. 3.

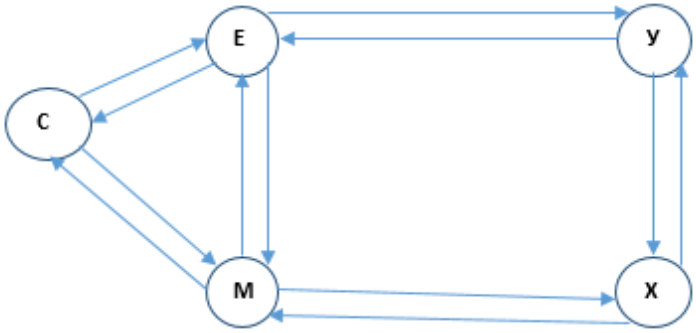


Рис. 3. Топология сети декаметровой радиосвязи (пример)

В сети 12 направлений связи. Для упрощения будем полагать одинаковое качество прохождения сигнала на встречных направлениях (что не всегда имеет место), объединяя их в одно направление. Упорядочим их номера следующим образом: 1 – *МС* (*СМ*), 2 – *МЕ* (*ЕМ*), 3 – *СЕ* (*ЕС*), 4 – *МХ* (*ХМ*), 5 – *ЕУ* (*УЕ*), 6 – *ХУ* (*УХ*). В матрице *P* индекс направления будет меняться сверху вниз, а индекс рабочей частоты – слева направо. На сеть выделено 9 рабочих частот. В примере будем полагать, что обмен во всех направлениях ведется только на одной скорости, то есть $N_v = 1$. Это позволит представлять матрицы *P* двумерными. Данную сеть можно масштабировать как по рабочим частотам, добавлением дополнительных, рядом расположенных по спектру частот, так и по направлениям связи, полагая возможность одновременного параллельного установления соединений между радиоцентрами.

Следует определить четыре возможных типа матриц *P* (*d, f, V*).

Тип 1: радиосеть изотропна по направлениям и радиоканалам. *P* (*d, f, V*) = *P* (*V*) для всех *d* и *f*. Ситуация типична для работы радиосети с антеннами зенитного излучения (АЗИ) на дальности до 600 км на частотах 2...8 МГц или для работы радиосети при отсутствии прогноза по оценке качества радиоканалов. Это может иметь место при отсутствии службы ИВ ЧДС или невозможности достоверного прогноза вследствие чрезвычайных условий. Именно для такого типа сети, были созданы классические алгоритмы множественного доступа, и разработаны протоколы ССР. Возможный вид матрицы *P* (пример):

$$P(d,f,1) = \begin{vmatrix} 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \end{vmatrix}.$$

Тип 2: радиосеть изотропна по направлениям и анизотропна по частотам. *P* (*d, f, V*) = *P* (*f, V*) для всех *d*. Ситуация типична для работы сети из двух групп абонентов, имеющих локальные области расположения, в которых они связаны между собой альтернативными каналами: провод, оптоволокно, УКВ и прочее. Типичным примером является взаимодействие двух АСУ, разделенных в пространстве: группировка МЧС в районе локального бедствия, взаимодействующая со штабом; группа надводных кораблей в походе, взаимодействующая со штабом флота и прочее.

Возможный вид матрицы *P* (пример):

$$P(d,f,1) = \begin{vmatrix} 0{,}4 & 0{,}6 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}1 & 0{,}4 & 0{,}7 & 0{,}9 \\ 0{,}4 & 0{,}6 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}1 & 0{,}4 & 0{,}7 & 0{,}9 \\ 0{,}4 & 0{,}6 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}1 & 0{,}4 & 0{,}7 & 0{,}9 \\ 0{,}4 & 0{,}6 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}1 & 0{,}4 & 0{,}7 & 0{,}9 \\ 0{,}4 & 0{,}6 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}1 & 0{,}4 & 0{,}7 & 0{,}9 \\ 0{,}4 & 0{,}6 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}1 & 0{,}4 & 0{,}7 & 0{,}9 \end{vmatrix}.$$

Тип 3: радиосеть изотропна по частотам и анизотропна по направлениям. $P\ (d,\ f,\ V) = P\ (d,\ V)$ для всех f. Это разновидность радиосети типа 1 при наличии сосредоточенных по направлениям помех искусственного или естественного происхождения. Возможный вид матрицы P (пример):

$$P(d,f,1) = \begin{vmatrix} 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 \\ 0{,}9 & 0{,}9 & 0{,}9 & 0{,}9 & 0{,}9 & 0{,}9 & 0{,}9 & 0{,}9 & 0{,}9 \\ 0{,}5 & 0{,}5 & 0{,}5 & 0{,}5 & 0{,}5 & 0{,}5 & 0{,}5 & 0{,}5 & 0{,}5 \\ 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 & 0{,}4 \\ 0{,}7 & 0{,}7 & 0{,}7 & 0{,}7 & 0{,}7 & 0{,}7 & 0{,}7 & 0{,}7 & 0{,}7 \end{vmatrix}.$$

Тип 4: сеть анизотропна по направлениям и частотам (общий случай). Степень анизотропии существенно влияет на эффективность функционирования сети. Гипотетически возможны варианты фрагментации сети на несколько независимых подсетей или направлений радиосвязи: для различных групп направлений связи все рабочие частоты различны. Возможный вид матрицы P (пример):

$$P(d,f,1) = \begin{vmatrix} 0{,}8 & 0{,}9 & 0{,}8 & 0{,}7 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 \\ 0{,}7 & 0{,}8 & 0{,}9 & 0{,}9 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 \\ 0{,}9 & 0{,}7 & 0{,}7 & 0{,}8 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 \\ 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}4 & 0{,}3 & 0{,}5 & 0{,}0 & 0{,}0 \\ 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}6 & 0{,}4 & 0{,}5 & 0{,}0 & 0{,}0 \\ 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}0 & 0{,}9 & 0{,}8 \end{vmatrix}.$$

Для различных групп направлений связи пригодны различные частоты. Физика данного явления может объясняться просто. Области отражения трасс для первой группы радионаправлений {1, 2, 3} находятся в одном районе. Все трассы односкачковые с примерно одинаковыми дальностями. Текущее время – день. Оптимальные частоты будут лежать в одном участке спектра от 9 до 16 МГц. Радионаправления второй группы {4, 5} имеют большую протяженность трасс. Для них оптимальными будут частоты выше 20 МГц. Радионаправление(я) третьей группы {6} находится в другом районе. Для него текущее время – ночь. Оптимальны частоты от 2 до 9 МГц.

Нулевая вероятность установления соединения за пределами указанных диапазонов в трех выделенных группах радионаправлений – некоторая натяжка, преднамеренно внесенная в данный пример для иллюстрации влияния анизотропии рабочих частот в рассматриваемой радиосети. Тем не менее, приведенный вид матрицы P четвертого типа фактически указывает, что в сети должны готовиться три комплекта радиоданных, назначаемых для различных групп направлений связи. Для радиоцентра M должны назначаться радиоданные 1 и 2 групп, для радиоцентра С – только первой группы, для радиоцентра $У$ – 2 и 3 групп.

2.3 Нагрузка и требования к её обслуживанию

Поступающая в сеть нагрузка определяется следующими параметрами. Среднее число сообщений, поступающих в сеть в единицу времени (слот) $0 \le A_m \le D_d$, нормированное число сообщений $0 \le \lambda \le 1$, где $\lambda = A_m / D_d$. Поток сообщений стохастический без памяти, направление передачи данных, в которое поступает сообщение, выбирается случайно. Закон распределения времени между окончанием и возникновением сообщений – геометрический (экспонента в дискретном времени). Математическое ожидание и дисперсия длин сообщений, нормированные по длине пакета – M_m и D_m. Требуемое время доставки пакета в сети – T_d. Требуемая вероятность доставки пакета в сети – P_r. Множество параметров, описывающих нагрузку в сети и требования к её обслуживанию, определяется как $\beta = (A_m, M_m, D_m, T_d, P_r)$.

2.4 Выбор группы рабочих частот и алгоритм множественного доступа

Назначение радиоданных: закрепление ГРЧ за направлениями передачи или подсетями в рассматриваемой радиосети и АМД целесообразно рассматривать и оптимизировать совместно.

В рассматриваемой технологии ППРЧ из комплекта F_S из F_c частот для каждого направления передачи d производится упорядоченная выборка пакета рабочих частот FB_d, в котором на первых местах находится F_b (d) стартовых частот, на которых происходит установление сеансов связи. Радиоданные сети определяют множество упорядоченных выборок частот, с указанием количества стартовых частот $FB = \{FB_k, F_k\}$, $k \in \{1,\ldots, N_f\}$, где N_f – количество ГРЧ в сети, которое может меняться от 1 до D_d. Если комплекты FB_d и FB_g совпадают для $d \neq g$, то направления d и g работают на одной ГРЧ. Если не совпадают, то эти направления находятся в разных ГРЧ. Как было указано выше в п. 1.1, F_d и наличие защитного интервала определяет, сколько радиоканалов может одновременно работать в ГРЧ с номером k.

Предлагается рассмотрение двух вариантов построения АМД.

Вариант 1: метод доступа с контролем занятости (МДКЗ) [3]. Процедура доступа состоит в разделении канала доступа на N_k каналов и выбора P_u вероятности занятия свободного канала. Приёмники радиостанций должны контролировать все каналы. При возникновении заявки на установление соединения, радиостанция выбирает один из свободных каналов, и с вероятностью P_u принимает решение о его занятии до начала слота. Если решение отрицательное, то в этом же временном слоте выбирается следующий свободный канал. Процедура повторяется до последнего свободного канала. В случае отрицательного результата, станция доступа ожидает следующий слот, и процедура повторяется. Возникновение коллизии, то есть столкновения пакетов различных станций определяется по отсутствию квитанции об установлении соединения со стороны вызываемого абонента. После детектирования коллизии процедура возобновляется.

МДКЗ обеспечивает высокую производительность сети в условиях взрывной и регулярной нагрузки. Его производительность (доля обслуженной нагрузки) для любого трафика выше 0,868 [3]. Это характеристика жесткого МДКЗ, без адаптивного снижения P_u при возникновении пучностей трафика. Гибкий МДКЗ с большей производительностью не рассматривается, ввиду произвольного увеличения в нем времени занятия канала. При малых нагрузках и большом числе свободных каналов велика вероятность немедленного занятия. При высоких нагрузках вероятность занятия автоматически становится меньше. Во всех случаях вероятность коллизии невысока.

Вариант 2: метод доступа «Радио-АТС», широко используемый в системах спутниковой связи. Метод подразумевает выделение из N_k каналов служебного канала для передачи заявок на установление соединения в режиме множественного доступа по протоколу *CSMA-CD* (*Carrier Sense Multiple Access with Collision Detection*) с настойчивостью занятия P_u и последующим детерминированным предоставлением свободного рабочего канала на время сеанса. Радиостанции наблюдают в эфире только служебный (вызывной) канал. Свободный рабочий канал определяется вызывающей радиостанцией. При занятости всех рабочих каналов, может быть разрешено использование служебного канала как рабочего на один сеанс. В процессе сеанса связи вызывающая станция обязана контролировать процесс освобождения рабочих каналов для перехода в первый освободившийся рабочий канал и предотвращение блокировки фрагмента сети на данной ГРЧ.

Для начала сеанса связи должно произойти два события: занятие служебного канала, верное детектирование наличия свободного рабочего канала для его использования. Производительность такой системы растет с увеличением длительности сеансов связи, с её уменьшением она снижается до производительности жесткого варианта протокола *CSMA-CD* – 0,531. Гибкий *CSMA-CD* или МДКН в терминах работы [3] имеет производительность выше до 0,81, однако, не рассматривается ввиду произвольного увеличения в нем времени занятия канала.

Априорно представляется, что МДКЗ имеет преимущество перед системой радио-АТС. В сети радиосвязи указанные выше параметры АМД определяются следующим образом: радиостанция при работе в направлении d может занять один из N_k свободных радиоканалов, образуемых k ГРЧ, назначенной для обслуживания данного направления. Интенсивность занятия определяется вероятностями $P_u = \{P_u(k)\}$, $k \in \{1,\ldots, N_f\}$, оптимизируемыми для каждой ГРЧ. В процессе установления и ведения связи в каждом направлении связи, частоты могут заменяться независимо, однако, число используемых частот для каждого направления остается прежним.

Таким образом, множество параметров алгоритма множественного доступа и назначения радиоданных есть $\gamma = (FB, P_u)$. Эти параметры являются предметом оптимизации.

3 Оценка эффективности функционирования сети декаметровой радиосвязи с ППРЧ

Для оценки эффективности функционирования сети представляется достаточным использование следующих показателей качества.

1) Вероятность своевременной доставки пакета в направлении d за требуемое время

$$P_d(\alpha, \beta, \gamma, \delta) = P_f(\beta) * P_c(\alpha, \beta, \gamma, \delta) * P_d(\alpha, \beta, \delta),$$

где $P_f(\beta)$ – вероятность наличия свободного канала при возникновении заявки за требуемое время,

$P_c(\alpha, \beta, \gamma, \delta)$ – вероятность установления соединения в направлении,

$P_d(\alpha, \beta, \delta)$ – вероятность отсутствия разрыва соединения за время передачи пакета.

2) Производительность сети $P_n(\alpha, \beta, \gamma, \delta) \in [0,1]$ – доля пакетов, переданных своевременно.

В соответствии с методом выбора доминирующего показателя качества, наиболее обоснованным представляется выбор производительности сети в качестве показателя эффективности функционирования сети радиосвязи при ограничении на вероятность своевременной доставки пакета:

$$P_n(\alpha, \beta, \gamma, \delta) = \frac{1}{D_d} \max_{0 \le \lambda \le 1} \sum_{d=1}^{D_d} \frac{1}{V(\alpha,\delta) T_m(\alpha,\beta,\gamma,\delta)}, \text{ если} P_d(\alpha, \beta, \gamma, \delta) \ge P_d \forall d,$$

где $T_m(\alpha, \beta, \gamma, \delta)$ – среднее время доставки пакета в направлении d,

$V(\alpha, \delta)$ – скорость передачи в направлении d на выбранных частотах.

Это и есть формулировка задачи анализа рассматриваемой системы радиосвязи.

4 Задача оптимизации алгоритма множественного доступа и назначения радиоданных

Задача оптимизации параметров сети радиосвязи или задача синтеза состоит в определении:

$$\gamma^* = \arg \max_{\gamma \in Y} P_n(\alpha, \beta, \gamma, \delta), \text{ если } P_d(\alpha, \beta, \gamma, \delta) \ge P_d \forall d.$$

Заключение

Предложенный подход позволяет построить формализованную модель, направленную на решение задачи параметрического синтеза алгоритма множественного доступа и назначения радиоданных для сети декаметровой радиосвязи, функционирующей в режиме ППРЧ. Он разделяет группы параметров, описывающих структуру сети, среду передачи, поступающую нагрузку и, собственно, алгоритм множественного доступа и назначения радиоданных. Такое разделение позволяет, при необходимости, выполнить независимую корректировку исходных данных по любой из названных четырех составных частей.

Представлена общая формулировка задач анализа и синтеза рассматриваемой системы связи, которая является методической основой для построения математической модели функционирования и разработки методики оптимизации параметров алгоритма множественного доступа и назначения радиоданных в сети декаметровой радиосвязи, функционирующей в режиме ППРЧ.

На основе общей формулировки возможна постановка частных задач, например:

- задачи построения сети, использующей только одну ГРЧ;
- задачи построения сети с постоянно закрепленными за направлениями радиоканалами ГРЧ;
- задачи оптимизации радиоданных при заранее заданном алгоритме множественного доступа;
- рассмотренной выше задачи оптимизации с ограничениями по дополнительно вводимым показателям качества функционирования сети.

Отдельному подробному рассмотрению подлежат возможные варианты:

- поиска и определения ключевой для данной работы матрицы $P(d, f, V)$;
- решения рассмотренной задачи оценки эффективности функционирования сети декаметровой радиосвязи с ППРЧ;
- решения приведенной выше задачи совместной оптимизации алгоритма множественного доступа и назначения радиоданных.

Литература

1. Recommendation ITU-R F.1487 Testing of HF modems with bandwidths of up to about 12 kHz using ionosfpheric cannel simulators, 2000: [Электронный ресурс]. URL: https://www.itu.int.

2. Путилин А.Н. Модель взаимодействия линии радиосвязи и станции радиоэлектронного подавления / Доклад на конф. «Региональная информатика-2012», 24-26 октября 2012 г. – СПб.: СПОИСУ, 2012.

3. Бунин С.Г., Войтер А.П. Вычислительные сети с пакетной радиосвязью. - Киев: Тэхника, 1989. - 129 с.

4. Хвостунов Ю.С. Реализации сетевой синхронизации в автоматизированной сети радиосвязи декаметрового диапазона. Техника средств связи. 2020. № 2 (150). С. 63-70.

5. Путилин А.Н., Хвостунов Ю.С. Концепция телекоммуникационной технологии сети дальней радиосвязи // Материалы XI Санкт-Петербургской Международной конференции «Региональная информатика-2010», Санкт-Петербург, 20-22 октября 2010 г.

6. Гук И.И., Путилин А.Н., Сиротинин И.В., Хвостунов Ю.С. Адаптивная система декаметровой радиосвязи с полнодиапазонной псевдослучайной перестройкой рабочей частотой. Предварительные результаты трассовых испытаний ее фрагмента // Материалы VI Санкт-Петербургской Межрегиональной конференции «Региональная информатика-2011», Санкт-Петербург, 26-28 октября 2011 г.

References

1. Recommendation ITU-R F.1487 Testing of HF modems with bandwidths of up to about 12 kHz using ionosfpheric cannel simulators, 2000: URL: https://www.itu.int.

2. Putilin A.N. *Model' vzaimodejstviya linii radiosvyazi i stancii radioelektronnogo podavleniya* [Model of interaction between a radio communication line and an electronic suppression station]. Report on the conf. "Regional Informatics 2012," October 24-26, 2012 - St. Petersburg: SPOISU, 2012 (in Russian).

3. Bunin S.G., Voiter A.P. *Vychislitel'nye seti s paketnoj radiosvyaz'yu* [Computing networks with packet radio communication] - Kiev: Tehnika, 1989. - 129 s. (in Russian).

4. Khvostunov Yu.S. *Realizacii setevoj sinhronizacii v avtomatizirovannoj seti radiosvyazi dekametrovogo diapazona* [Implementation of network synchronization in the automated radio network of the decameter range]. Means of communication equipment. 2020. No 2 (150). Pp. 63-70 (in Russian).

5. Putilin A.N., Khvostunov Yu.S. *Koncepciya telekommunikacionnoj tekhnologii seti dal'nej radiosvyazi* [Concept of telecommunications technology of long-distance radio communication network]. Materials of the XI St. Petersburg International Conference "Regional Informatics" RI-2010, "St. Petersburg, October 20-22, 2010 (in Russian).

6. Guk I.I., Putilin A.N., Sirotinin I.V., Khvostunov Yu.S. *Adaptivnaya sistema dekametrovoj radiosvyazi s polnodiapazonnoj psevdosluchajnoj perestrojkoj rabochej chastotoj. Predvaritel'nye rezul'taty trassovyh ispytanij ee fragmenta* [Adaptive system of decameter radio communication with full-range pseudo-random rearrangement of working frequency. Preliminary results of track tests of its fragment]. Materials of the VI St. Petersburg Interregional Conference "Regional Informatics" RI-2011, "St. Petersburg, October 26-28, 2011 (in Russian).

Статья поступила 05 августа 2020 г.

Информация об авторах

Панин Роман Сергеевич – Адьюнкт Военной академии связи им. Маршала Советского Союза С.М.Буденного. Тел.: +7 (952) 373-50-71. E-mail: Zzz822@mail.ru.

Путилин Алексей Николаевич – Доктор технических наук, профессор. Главный научный сотрудник научно-технического центра ПАО «Интелтех». Тел.: +7 (812) 448-19-01. E-mail: PutilinAN@inteltech.ru.

Хвостунов Юрий Сергеевич – Кандидат технических наук. Заместитель начальника научно-технического центра ПАО «Интелтех». Тел.: +7 (812) 448-96-30. E-mail: HvostunovYS@inteltech.ru.

Use of frequency resource by decameter communication system in pseudorandom operation frequency tuning mode

R.S.Panin, A.N. Putilin, Yu.S. Khvostunov

Annotation. *The article deals with the formulation of the problem of joint optimization of the choice of operating frequencies and parameters of the multiple access algorithm for a decameter communication network. The mode of frequency-hopping spread spectrum (FHSS) with time-frequency separation of radio channels of different subscribers is investigated. In radio communication systems with FHSS, there is no traditionally used assignment of operating frequencies to radio lines, which makes the existing methods of assigning operating frequencies ineffective. The aim of this work is to formulate the problem of joint optimization of operating frequencies and parameters of the multiple access algorithm in the decameter radio network. Theoretical and practical groundwork in the field of digital data transmission over a decameter communication channel is used. The novelty of the work consists in the formulation of the problem of joint optimization of the choice of operating frequencies and parameters of multiple access algorithms. The practical result of the work is determined by the emerging possibility of automating the process of preparing radio data in an automated communication control system. Also, the group use of frequencies provides a significant increase in the efficiency of the decameter radio network.*

Keywords: *decameter radio communication; pseudorandom tuning of the operating frequency; frequency resource; multiple access algorithm.*

Information about authors

Panin Roman Sergeevitch - Adjunct of the Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. Tel. +7 (952) 373-50-71. E-mail: Zzz822@mail.ru.

Putilin Alexey Nikolaevith - Doctor of technical Sciences, Professor. Chief research officer of the scientific and technical center of PJSC «Inteltech». Tel.: +7 (812) 448-19-01. E-mail: PutilinAN@inteltech.ru.

Khvostunov Yuri Sergeevith - Candidate of technical Sciences. Deputy head of the scientific and technical center of PJSC «Inteltech». Tel.: +7 (812) 448-96-30. E-mail: HvostunovYS@inteltech.ru.

Для цитирования: Панин Р.С., Путилин А.Н., Хвостунов Ю.С. Использование частотного ресурса системой декаметровой связи в режиме псевдослучайной перестройки рабочей частоты // Техника средств связи. 2020. № 3 (151). С. 2-13.

For citation: Panin R.S., Putilin A.N., Khvostunov Yu.S. Use of frequency resource by decameter communication system in pseudorandom operation frequency tuning mode. Means of communication equipment. 2020. No 3 (151). Pp. 2-13 (in Russian).

УДК 621.391

Особенности построения рациональной структуры транспортной сети ведомственной телекоммуникационной системы

Курносов В.И., Лукин К.И.

Аннотация. *Рассматривается обобщенный подход к синтезу полиструктуры ведомственной телекоммуникационной системы. Показано, что последовательность ведомственной телекоммуникационной системы будет носить итерационный (многошаговый) характер и может быть представлена в виде поэтапного решения отдельных задач с использованием частных методик. Предлагается в рамках общей последовательности решения целевой задачи выбрать (обосновать) основные алгоритмы реализации, которые позволят построить структуру ведомственной телекоммуникационной системы, обеспечивающую её устойчивое функционирование.*

Ключевые слова: *телекоммуникационная система; единая транспортная сеть; информационное направление связи; комплекс аппаратно-программных средств; топологическая структура.*

Как показывают исследования, характер и особенности функционирования ведомственной телекоммуникационной системы (ВТКС) во многом будет определяться рациональностью построения ее топологической, потоковой и физической структур. Особо актуален данный вопрос для ВТКС, в которой совокупный сетевой ресурс формируется в интересах выполнения эксплуатационных норм в различных плоскостях ее полиструктуры.

Анализ, проведенный в [1], показывает, что для решения задачи построения единой транспортной сети ВТКС целесообразно использовать логико-аналитический метод формирования её структуры. Особенность данного метода, по сравнению с другими, состоит в том, что он позволяет из ограниченного множества структур, найденных посредствам аналитических соотношений, выбрать конкретный вариант в соответствии с целевым предназначением ВТКС, уровнем дестабилизирующих воздействий на избыточность их структуры, квалификацией обслуживающего персонала и другими факторами, которые можно учесть, например, при имитационном моделировании.

В соответствии с [2] в общем случае рациональная структура ВТКС для выполнения заданных критериев должна строиться относительно плоскостей и уровней ее образующих. При этом с учетом того, что основу перспективной ВТКС будут составлять многосервисные, многопротокольные сети связи, структура такой системы должна формироваться совместно со специальными и обеспечивающими их эксплуатацию службами и системами: тактовой сетевой синхронизацией (ТСС), сигнализации (СС) и технической эксплуатации (ТЭ). Такой подход позволяет изначально учитывать сетевые ресурсы, закладываемые (необходимые) в топологическую, потоковую и физическую структуры ВТКС.

В этом случае последовательность построения ВТКС будет носить итерационный (многошаговый) характер и может быть представлена в виде поэтапного решения отдельных задач с использованием частных методик. Основу методик может составлять процесс обеспечения эксплуатационных норм в различных плоскостях, с последующим уточнением результатов каждой из них относительно предыдущих этапов.

Поэтому в рамках общей последовательности решения целевой задачи необходимо разработать совокупность методик и выбрать (обосновать) основные алгоритмы их реализации, которые позволят построить структуру ВТКС совместно со структурами обеспечивающих ТСС, СС и системы управления в условиях воздействия дестабилизирующих факторов.

При этом ВТКС будет рассматриваться как двухуровневая структура, состоящая из транспортной сети и сетей доступа. В то же время, исходя из условий функционирования ВТКС, ее транспортную компоненту целесообразно строить частично инвариантной по пропускной способности, а сети доступа – в виде зон по территориально-административному принципу.

В каждой зоне доступа целесообразно выделить корреспондирующие пары, образующие информационные направления связи (ИНС), принадлежащие данной зоне, а также корреспондирующие пары, образующие ИНС относительно разных зон доступа. Взаимоувязывание сетей доступа производится посредством единой транспортной сети.

При этом ресурс по качеству и пропускной способности, заложенный в инвариантную часть транспортной сети, должен обеспечить потребности служб синхронизации, сигнализации, управления ВТКС и пользователей I класса. Остальной требуемый сетевой ресурс в интересах пользователей II и III класса закладывается в безынтервальную часть транспортной сети ВТКС [3].

Для построения транспортной сети ВТКС, в качестве модели можно использовать многопродуктовую, многополюсную потоковую сеть. Эта модель при применении ресурсосберегающих КАПС (коллективного пользования, пакетной обработки, работы в реальном масштабе времени и т. п.) может быть представлена многопродуктовым графом *G* (*A, B, H, U*), в котором *A* – узловая основа сети, *B* – сетка линий сети, определяющая ребра между узлами сети, *H* – структурная надежность ребер сети, *U* – пропускная способность ребер сети [4]. В качестве исходных данных будем считать заданными следующее:

1) Совокупность пунктов управления Ф: $A_1 = \left\{a_i^{(1)}\right\}, \left\{x_i^{(1)}, y_i^{(1)}\right\}, \quad i = \overline{1, N_1}$, из которых формируются корреспондирующие пары

$Z = \{Z_k\}, \quad Z_k = \left\{a_{\rho_k}; a_{g_k}\right\}, \quad k = \overline{1, m}$, соответствующие информационным направлениям связи (ИНС).

2) Вектор $\vec{V} = \left[V_{Z_1}, ..., V_{Z_K}, ..., V_{Z_m}\right]^T$, компоненты которого определяют требуемые пропускные способности ИНС (могут быть заданы числом стандартных цифровых каналов для передачи информационных сообщений (ИС) с пропускной способностью 64 Кбит/с).

3) Вектор $\vec{H}^{(\text{Тр})} = \left[H_1^{(\text{Тр})}, ..., H_m^{(\text{Тр})}\right]^T$ определяющий требования к структурной надежности пучков каналов для $\{Z_K\}$ сети.

4) Требования к коэффициентам ошибок и фазовым дрожаниям сетевых каналов $\left\{k_{\text{ош}}^{(\ell)}; J_g^{(\ell)}\right\}, \ell = \overline{1, \gamma}$, где ℓ – вид услуги, предоставляемой пользователям.

5) Построение сети, которая реализуется с использованием совокупности цифровых систем передачи (ЦСП), образованных посредством технологий плезиохронных и синхронных цифровых иерархий, характеризуемых:

$$\left\{\vec{n}^{\mu}, \alpha_{\mu}, \beta_{\mu}, \gamma_{\mu}, \vec{V}_{\mu}, \vec{L}_{\mu}, \vec{H}_{\mu}, \vec{\Psi}_{\mu}\right\}, \quad n = 1, ..., Q; \quad \mu = 1, ..., M,$$

где $\vec{n}^{\mu}$ – тип ЦСП из заданного ряда от 1 до *Q*; $\alpha_{\mu}, \beta_{\mu}, \gamma_{\mu}$ – коэффициенты, по которым рассчитывается приведенная стоимость ЦСП и их участков в ВТКС; $\vec{V}_{\mu}$ – вектор пропускных способностей, реализуемых ЦСП; $\vec{L}_{\mu}$ – вектор, определяющий структуру цифровой линии передачи; $\vec{H}_{\mu}$ – вектор надежности ЦСП; $\vec{\Psi}_{\mu}$ – вектор эксплуатационных норм на параметры цифровых каналов передачи (связи).

Совокупность ЦСП позволяет сформировать узловой ресурс $R_{\text{у}} = \left\{r^{\nu}\right\}, \ \nu = \overline{1, Q_{\text{у}}}$, где r – тип узла и линейный ресурс сети $R_{\text{л}} = \left\{r^{\chi}\right\} \ \chi = \overline{1, Q_{\text{л}}}$. Узловой ресурс определяет

коммутационные возможности, надежность оборудования, затраты на развертывание и эксплуатацию узлов сети. Посредством линейного ресурса реализуется сетка линий ВТКС. На транспортной сети ВТКС используется принудительная иерархическая сетевая тактовая синхронизация со структурной надежностью передачи сигналов синхронизирования $\eta = H_{1,j}$, $j = \overline{2,N}$.

Задачу построения единой транспортной сети ВТКС целесообразно решать в виде последовательности частных задач, с корректировкой решений на отдельных этапах посредством имитационной модели для их взаимной увязки. При этом на первом этапе проводится синтез ее топологической структуры, которая должна обеспечивать ресурс сети по качеству каналов, структурной надежности при передаче как информационных, так и сигнально-управляющих потоков информационных сообщений. Полученная топологическая структура будет являться основой для формирования потоковой структуры с определением пропускных способностей ребер сети и распределением потоков по ним. Сформированные таким образом топологическая и потоковые структуры обеспечат принятие решения по построению физической структуры транспортной сети ВТКС путем решения задачи выбора из заданного дискретного ряда технических средств с рациональной расстановкой соответствующего оборудования КАПС на узлах ВТКС.

В соответствии с рассмотренными этапами решения задачи, ее последовательность может быть представлена в виде следующего алгоритма.

1) Нахождение числа и местоположения узлов доступа ВТКС $A_{\text{Д}}^{(D)} = \{a_{i_g}\}, \{x_{i_g}, y_{i_g}\}, i_g = \overline{1, N_g}$.

2) Составление матрицы тяготения между узлами доступа $\{Z_k\}_{g_\ell}$, $\{U_k\}_{g_\ell}$, $\ell = \overline{1, m_1}$.

3) Составление матрицы связности между узлами доступа $(h_{\text{св}})_{g_\ell}$. Выбор максимального значения $h_{\text{св}}$ между узлами доступа.

4) Определение требований к рангам сетевых узлов единой транспортной сети $r(a_i) = \max\{h_{\text{св}}\}_{g_\ell}$.

5) Построение узловой основы транспортной сети.

6) Построение сетки ребер транспортной сети ВТКС (нахождение числа и местоположения ребер сети) $B = \{b_{ij}\} = \{b_1, ..., b_n\}$.

7) Построение инвариантной части по пропускной способности транспортной сети ВТКС.

8) Построение безынтервальной части транспортной сети ВТКС.

9) Уточнение пропускной способности ребер ВТКС относительно существующего и планируемого к развертыванию парка ЦСП.

10) Распределение систем передачи и оборудования узлов коммутации ВТКС.

В дальнейшем, решение задачи направлено на построение топологической структуры транспортной сети ВТКС. При этом, с позиции оптимизации транспортных сетей связи и выполнения ими всех требований по переносу ИС, представляют интерес топологические структуры однородных сетей, то есть сетей абсолютной однородности или имеющих минимальную неоднородность. Такие структуры допускают реализацию всех известных в современной технике режимов функционирования КАПС, видов управления сети (иерархического, децентрализованного и др.), способов обработки информации, формирование разветвленных неиерархических структур. Структуры максимальной однородности или имеющие минимальную неоднородность наиболее адекватны решаемым задачам построения транспортной сети, т. к. допускают разбиение на функционально независимые части, адаптацию к внешним условиям и к требованиям пользователей сети [5].

Наращиваемость таких структур осуществляется без изменений в первоначальном ее составе. Определив потоковую структуру транспортной сети ВТКС, можно приступить к построению ее физической структуры, которая связана с расстановкой систем передачи, в том числе используемых в ресурсосберегающих КАПС, на сетевых узлах. В данном случае задача решается с учетом пригодности прохождения трасс по физико-географическим условиям и дестабилизирующим воздействиям, обеспечения отказоустойчивости ребер и эффективного использования энергетики линий передачи на путях прохождения каналов. Для решения данной задачи целесообразно использовать метод последовательного анализа вариантов, который достаточно подробно рассмотрен в [6].

Выводы

Синтезированная вышерассмотренным образом сеть позволяет осуществить распределение каналов в данный момент времени в соответствии с заданными требованиями по пропускной способности и обеспечить структурную надежность ВТКС. Кроме того, построенная таким образом структура ВТКС является уницентральной, что позволяет более эффективно развертывать на ней систему связи и сети обмена данными в интересах ведомства. Однако сформированная выше приведенным способом структура ВТКС не конкретизирована относительно особенностей построения обеспечивающих плоскостей ее полиструктуры. Поэтому дальнейшим направлением решения задачи в целях выполнения требований к устойчивости функционирования ВТКС должно являться разработка методики формирования ее тактовой сетевой синхронизации.

Литература

1. Жигадло В.Э. Архитектура телекоммуникационных сетей. – СПб.: ВУС, 2000. – 218 с.

2. Курносов В.И. Методологические аспекты формирования технического облика перспективных телекоммуникационных систем // Труды межведомственного НТС «Технология общесистемных работ в области телекоммуникаций». – СПб.: ОАО НИИ «Звезда», 2000. – С. 31-37.

3. Военные системы многоканальной электросвязи. Часть II. Учебн. пособие. Под ред. Лебедева А.Т. – Л.: ВАС, 1992. – 269 с.

4. Филин Б.П. Методы анализа структурной надежности сетей связи. – М.: Радио и связь, 1998. – 211 с.

5. Вторичные сети военной связи. Бабошин В.А., Керко В.А., Лисовский А.В. и др. Под ред. А.В. Лисовского. – М.: Изд-во МО РФ, 2002. – 591 с.

6. Калихман И.Л., Войтенко М.А. Динамическое программирование в примерах и задачах: Учеб. пособие. – М.: Высшая школа, 1989. – 125 с.

References

1. Zhigadlo V.E. Architecture of telecommunication networks. - St. Petersburg. VUS, 2000. - 218 p. (in Russian).

2. Kurnosov V.I. Methodological aspects of the formation of the technical appearance of promising telecommunications systems. Proceedings of the interdepartmental NTS "Technology of system-wide work in the field of telecommunications". St. Petersburg. JSC Research Institute "Zvezda", 2000. p. 31-37 (in Russian).

3. Military systems of multichannel telecommunications. Part II. Training manual. Ed. Lebedeva A.T. Leningrad. VAS, 1992. 269 p. (in Russian).

4. Filin B.P. Methods of analysis of structural reliability of communication networks. Moscow. Radio and communication, 1998. 211 p. (in Russian).

5. Secondary military communication networks. Baboshin V.A., Kerko V.A., Lisovsky A.V., etc. Edited by A.V. Lisovsky. Moscow. Publishing House of the Ministry of Defense of the Russian Federation, 2002. 591 p. (in Russian).

6. Kalikhman I.L., Voitenko M.A. Dynamic programming in examples and problems. Textbook. Moscow. Higher School, 1989. 125 p. (in Russian).

Статья поступила 13 августа 2020 г.

Информация об авторах

Курносов Валерий Игорьевич – Доктор технических наук. Ведущий специалист ПАО «Интелтех». Тлф.: +7 (921) 303-21-05. E-mail: vi-kurnosov@mail.ru. Адрес: 197342, Россия, Санкт-Петербург, Кантемировская ул., д. 8.

Лукин Константин Игоревич – Кандидат технических наук. Генеральный директор ОАО «Супертел». Тлф.: +7 (812) 232-73-21. E-mail: info@supertel.ru. Адрес: 197101, Россия, Санкт-Петербург, Петроградская наб., д. 38 А.

Features of building a rational structure of the transport network of the departmental telecommunication system

V.I. Kurnosov, K.I. Lukin

Annotation. *A generalized approach to the synthesis of the polystructure of a public telecommunication system is considered. It is shown that the sequence of construction of a public telecommunication system will be iterative (multi-step) in nature and can be represented as a step-by-step solution of individual problems using particular techniques. It is proposed to select (justify) the main implementation algorithms within the general sequence of solving the target problem, which will allow to build the structure of a public telecommunication system, ensuring its stable functioning.*

Keywords: *telecommunication system, unified transport network, information direction of communication, complex of hardware and software, topological structure.*

Information about the Authors

Valery I. Kurnosov – Doctor of Technical Sciences. Leading Specialist of PJSC "Inteltech". Tel.: +7 (921) 303-21-05. E-mail: vi-kurnosov@mail.ru. Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya street, 8.

Konstantin I. Lukin – Candidate of Technical Sciences. General Director of JSC "Supertel". Tel.: +7 (812) 232-73-21. E-mail: info@supertel.ru. Address: Russia, 197101, Saint-Petersburg, Petrogradskaya nab., 38A.

Для цитирования: Курносов В.И., Лукин К.И. Особенности построения рациональной структуры транспортной сети ведомственной телекоммуникационной системы // Техника средств связи. 2020. № 3 (151). С. 14-18.

For citation: Kurnosov V.I., Lukin K.I. Features of construction of rational structure of transport network of departmental telecommunication system. Means of communication equipment. 2020. No 3 (151). Pp. 14-18 (in Russian).

УДК 654.02

Протоколы O2П и O2M для переноса IP-трафика в низкоскоростных сетях с высоким коэффициентом ошибок

Егоров А.А.

Аннотация. *Предложены протоколы O2П и O2M для передачи Transmission Control Protocol/Internet Protocol-трафика и обеспечения динамической IP-маршрутизации в низкоскоростных сетях с высоким коэффициентом ошибок, в том числе, магистральных декаметровых радиосетях. Исследованы характеристики и режимы работы протоколов на макете сети в реальном масштабе времени. Приведены характеристики информационного обмена с использованием разработанных протоколов O2П и O2M при различных вероятностях потерь в канале связи.*

Ключевые слова*: протокол O2П; протокол O2M; передача данных; динамическая маршрутизация; коэффициент ошибок; низкоскоростная сеть; декаметровая и коротковолновая радиосвязь; Transmission Control Protocol / Internet Protocol.*

Введение

На сегодняшний день в мире растет потребление и, соответственно, генерация телекоммуникационных услуг, что требует увеличения пропускной способности магистральных, в основном наземных линий связи. Но, в тоже время, не теряет актуальности использование радиолиний декаметрового (ДКМВ) диапазона волн как возможной резервной системы при деградации наземных и спутниковых каналов связи [1].

Высокая дальность связи и устойчивость радиоэлектронному противодействию позволяет рассматривать коротковолновую (КВ) радиосвязь как один из способов построения резервных магистральных сетей в интересах Вооруженных сил Российской Федерации (ВС РФ). При этом требуется поддержать работу максимально возможного спектра услуг связи, в том числе услуги передачи данных по протоколу *Transmission Control Protocol, Internet Protocol* (*TCP*/*IP*).

Надежность радиосвязи ДКМВ диапазона определяется многими причинами, к важнейшим из которых относятся уровень принимаемого сигнала (соотношение сигнал/шум) и степень многолучевости, приводящая к возникновению замираний. Длительность замираний меняется в широких пределах в зависимости от характеристик радиотрасс, времени года и суток, частоты и ионосферных условий. В часы сильно развитой многолучевости, радиосвязь на этих радиотрассах может оказаться даже невозможной [2].

Практически полученные данные по унаследованным эфирным модемам показывают, что, при передаче бинарных данных, вероятность (коэффициент) ошибок (КОШ) в среднем составляет 10^{-3}, а скорость – 1200-2400 бит/с [3]. Однако, если искажения устраняются различными методами кодирования и декодирования передаваемых данных, то проблемы распространения радиосигнала, связанные с замираниями, не так легко решаются современным оборудованием и алгоритмами обработки. Длительные замирания радиосигналов в ионосферных слоях приводят к невозможности установления связи между абонентами (на уровне используемого ими транспортного протокола). В этом случае, необходимо организовать передачу данных к станции назначения через промежуточные сетевые узлы (радиоцентры) и рассчитывать оптимальный маршрут с использованием алгоритмов и протоколов динамической маршрутизации [4].

В то же время аналитические исследования работы протокола *IP* и *TCP* показывают, что нарушения обмена *TCP*-сессии наблюдаются при коэффициенте битовых ошибок более 10^{-4} [5, 6]. Таким образом, для решения проблем передачи *IP*-трафика через сеть ДКМВ-радиоканалов необходим протокол (семейство протоколов), способный перенести *IP*-трафик

в режиме маршрутизации с точки входа в радиосеть в адресуемую точку выхода. Также в целях уменьшения служебного трафика, протокол должен иметь тесную интеграцию с протоколами динамической маршрутизации, в качестве анализатора канала связи для эффективного построения маршрутов в условиях нестабильности качества радиосети.

Помехоустойчивый протокол передачи данных О2П

Разработанный протокол О2П представляет собой протокол канального уровня, адаптирующийся к каналу связи как по скорости передачи, так и по его качеству (количеству ошибок), адаптацией многофакторной. В процессе передачи данных возможно изменение размеров передаваемых элементов и степени защиты информации восстанавливающими кодами. Также протокол обеспечивает контроль за линией по коэффициентам адаптации, что используется протоколами следующего уровня для обеспечения динамической маршрутизации.

В качестве транспортной сети для протокола О2П могут применяться протоколы различных физических линий (С1И, *Ethernet*, *RS*-232) или модемные соединения.

Протокол О2П предназначен для передачи поступающих в интерфейс маршрутизатора из *IP*-сети пакетов (блоков данных) длиной до 1500 байт с последующей обработкой и передачи их по низкоскоростным линиям связи с коэффициентом ошибок канала не более 10^{-2}. Особенностью протокола является малое количество служебных сообщений, что, во-первых, приводит к простой реализации, а во-вторых уменьшает количество таймированных состояний, когда, в случае потерь управляющих сообщений сторона вынуждена ожидать некоторое время, чтобы сменить свое состояние. Для обеспечения помехозащищенности в протоколе применяются коды Хемминга и кодирование Рида-Соломона [7]. Причем кодирование Рида-Соломона подключается автоматически, при необходимости.

Протокол работает по принципу заполнения приемного окна. Вначале передатчик отправляет служебное сообщение о намерениях передачи блока данных соответствующей длины. Приемник выделяет пустое окно необходимого размера и отправляет подтверждение о готовности принимать данные. После получения подтверждения, передатчик делит блок данных на сегменты, в соответствии с параметрами адаптации, и начинает их передачу. Передача сегментов осуществляется кумулятивным методом с адаптацией по количеству «одновременно» передаваемых сегментов. В зависимости от информации, содержащейся в служебных полях, в принимаемых сегментах приемник отправляет передатчику сообщения о пустых местах в приемном окне, которые могли образоваться в результате пропадания этих сегментов. Блок данных считается принятым, если от приемника пришло подтверждение с отсутствием пустых мест в окне, т. е. окно заполнено.

Сегменты снабжаются полем контрольной суммы, поэтому сегменты, которые не удалось откорректировать, в окно не попадают и считаются непринятыми. Размер сегмента изменяется передатчиком, в зависимости от «качества» приема, которое рассчитывается на основании сообщений приемника о заполненности окна.

Протокол имеет свой *High-Level Data Link Control (HDLC)*, что позволяет ему работать с байтовым потоком и выделять из него сообщения.

Помехоустойчивый протокол динамической маршрутизации О2М

Протокол динамической маршрутизации О2М применяется для передачи информации о характеристиках доступности узлов *IP*-сети пакетной передачи данных на низкоскоростных каналах связи с высоким коэффициентом ошибок. Протокол, преимущественно, используется совместно с протоколом О2П.

О2М может являться расширением протокола О2П, так как имеет общий формат заголовка, но может применяться и отдельно.

Протокол О2М позволяет обнаруживать топологию сети – определять *IP*-адреса включенных в сеть интерфейсов и их соединения. С помощью данного протокола узлы обмениваются метрическими стоимостями передачи пакета между портами узлов, там самым формируют и корректируют матрицу смежности, по которой уже строится таблица маршрутизации для каждого узла.

Размер обслуживаемых сетей протокола О2М достигает до 127 узлов, при этом на каждом узле может быть не более 31 порта. Протокол О2М позволяет работать в режиме «вскрытия» топологии радиосети, а также поддерживает балансировку нагрузки, перераспределяя трафик с нагруженных направлений на менее нагруженные.

В основе работы протокола лежит принцип широковещательной рассылки пакетов. Узел, получивший пакет О2М, соблюдая ряд условий, распространяет его по остальным своим интерфейсам. Размер пакета не более 17 байт, поля защищены кодом Хэмминга и закрыты контрольной суммой.

В протоколе О2М отсутствуют сеансовые обмены между узлами (когда узел вынужден ожидать ответа встречной стороны), вследствие этого обработчик протокола О2М не имеет таймированных состояний, что позволяет работать протоколу более эффективно на низкоскоростных каналах.

Оценка возможностей работы протоколов О2П/О2М

Оценка возможностей работы протокола О2П и О2М проводилась на макете сети, представленной на рис. 1 в режиме реального времени. Сеть образуют 5 макетов маршрутизаторов, соединенных между собой линиями *RS*-232. В разрыв линии включается имитатор радиоканалов (МИРЛ).

Макет IP-маршрутизатора представляет собой программно-аппаратное устройство на базе персонального компьютера, с установленными адаптерами *RS*-232. Программное обеспечение протоколов О2П/О2М и ядро стека *TCP*/*IP* функционирует под защищенной операционной системой реального времени (ЗОСРВ) КПДА.10964-01 «Нейтрино». Программная реализация протокола О2П образует в системе множество сетевых *IP*-интерфейсов, аналогичных сетевым *IP*-интерфейсам *Ethernet*. Каждый интерфейс О2П закреплен за физическим портом линии *RS*-232. Таким образом, *IP*-пакеты после маршрутизации в ядре стека *TCP*/*IP* поступают на соответствующий О2П интерфейс, где обрабатываются протоколом О2П и отправляются в физическую линию *RS*-232. Прием пакетов происходит аналогично в обратном порядке.

Имитаторы радиоканалов представляют собой многоканальный сервер с интерфейсами *RS*-232, любая пара из которых может образовывать имитатор дуплексной радиолинии. Программное обеспечение сервера имитаторов радиолиний позволяет вносить в каждый канал битовые (КОШ от 10^{-1} до $10^{-\infty}$) или серийные ошибки – отсутствие возможности работы по имитатору радиолинии сроком до 5 мин.

Для анализа работы протоколов в схему включены 2 имитатора нагрузки с программным обеспечением, реализующим мониторинг пропускной способности в реальном масштабе времени.

Для исследования работы протоколов О2П и О2М был сформирован план испытаний. Весь набор испытаний поделен на 2 группы, в зависимости от условий, возникающих в радиосети:

– первая группа испытаний проводилась в условиях статичной радиосети без имитации замираний, когда фиксировано задавались одинаковые по всем линиям связи значения коэффициентов ошибок;

– вторая группа испытаний проводилась в условиях динамичной радиосети с имитацией замираний, в этом случае на каждой «радиолинии» задавалось минимальное допустимое значение КОШ, случайным образом меняющимся во времени.

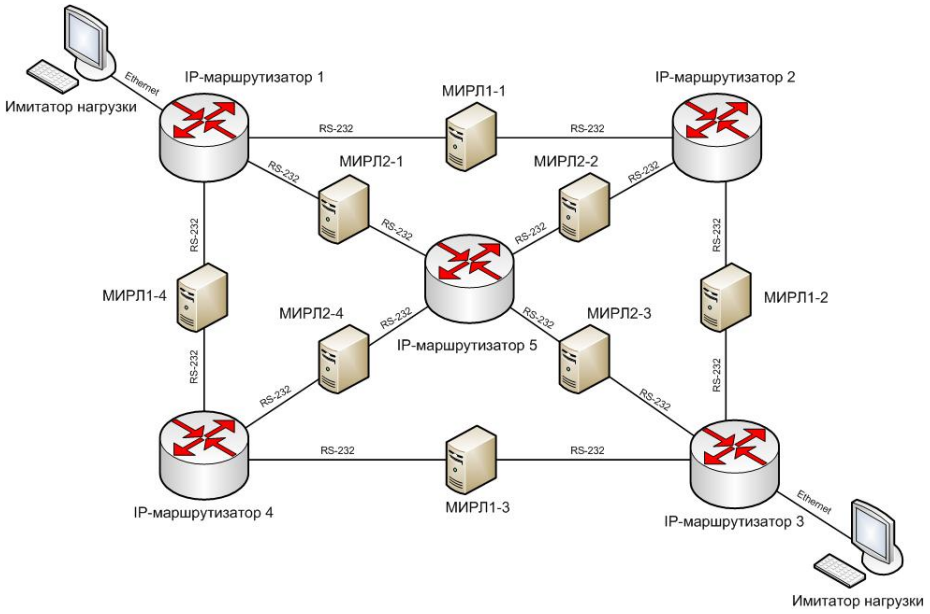


Рис. 1. Макет сети исследования протоколов О2П/О2М

В рамках каждой группы условий исследования передачи *IP*-пакетов проводились для различных типов *IP*-маршрутизации:

– при статической *IP*-маршрутизации без применения протокола О2М;

– при динамической *IP*-маршрутизации с применением протокола О2М, который позволял работать в режиме балансировки нагрузки.

Для каждой сессии измерений задавались скорости каналов сети: 1200, 2400, 4600, 9600 бит/с и базовые коэффициенты ошибок: 10^{-2}, $2*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}.

Измерения проводились для *TCP*-сессии, которую устанавливали между собой имитаторы нагрузок. При испытаниях в условиях статичной радиосети, измерения велись в течение передачи 1500 сообщений, по 100 байт в рамках одной *TCP*-сессии. В условиях динамичной радиосети (в условиях замираний), измерения проводились в течение 2-3 часов обмена сообщениями по одной *TCP*-сессии или, в ряде случаев, до получения обрыва *TCP*-сессии.

Полученные результаты измерений, в виде журналов статистики имитаторов нагрузки и радиолиний, а также дампы анализатора трафика *Wireshark*, объединялись и обрабатывались программными средствами, в том числе с помощью *MS Excel*.

Результаты работы протокола в условиях статичной сети

Работа протокола О2П на статичной радиосети без замираний и без применения протокола динамической маршрутизации О2М показывает довольно хорошие результаты. График зависимости информационной скорости *TCP*-обмена от коэффициента битовых ошибок на линии показан на рис. 2.

Благодаря помехоустойчивости протокола О2П, информационный обмен ведется на стабильной скорости в широком диапазоне коэффициентов ошибок от 10^{-5} до 10^{-3} . Так, при коэффициенте ошибок 10^{-3} и канальной скорости 1200 бит/с, средняя информационная скорость *TCP*-обмена составляет порядка 450 бит/с.

При самых худших условиях испытаний при высоком коэффициенте ошибок 10^{-2} и скорости канала в 1200 бит/с *TCP*-сессия устанавливается, и ведется обмен данными со скоростью не более 30 бит/с, но при таких скоростях возможны возникновения обрывов, так как появляются предельно высокие задержки для *TCP*-сессии.

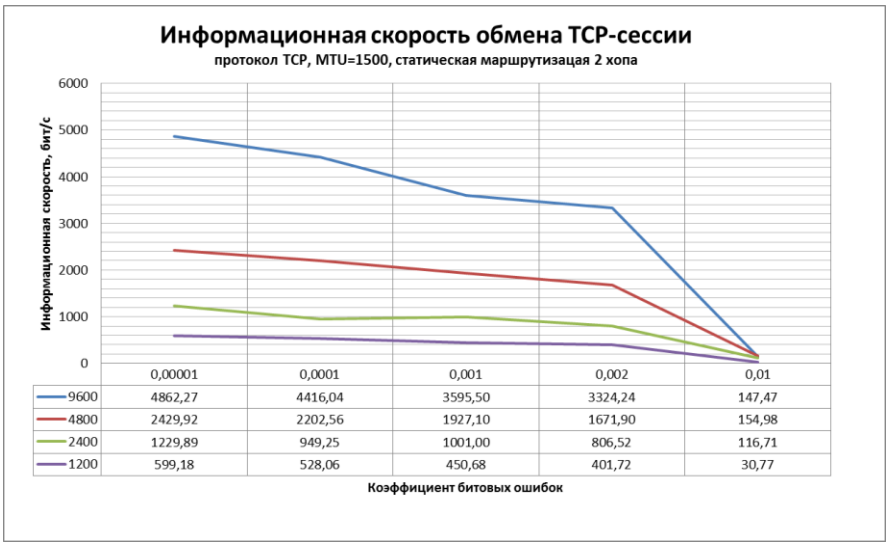


Рис. 2. Зависимость информационной скорости обмена *TCP* от КОШ

Процент служебного трафика О2П при различных КОШ и скоростях каналов показан на рис. 3.

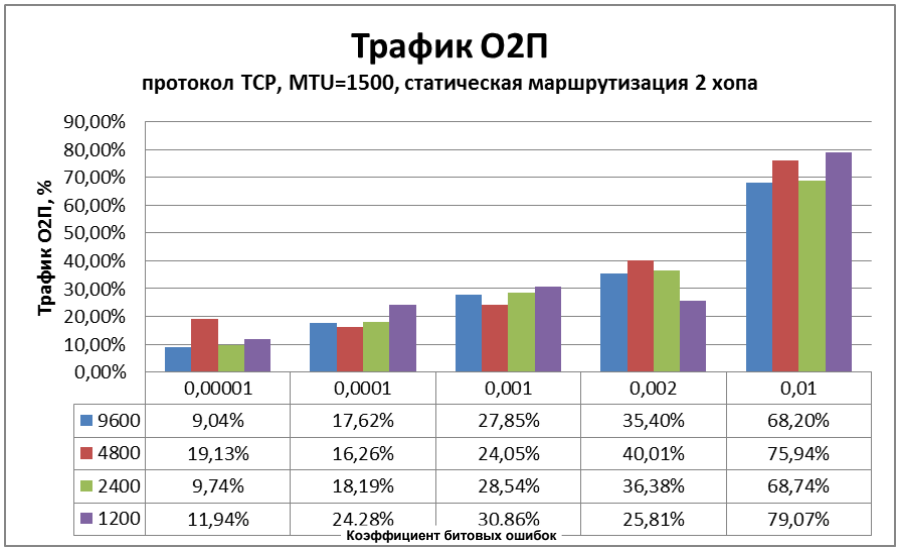
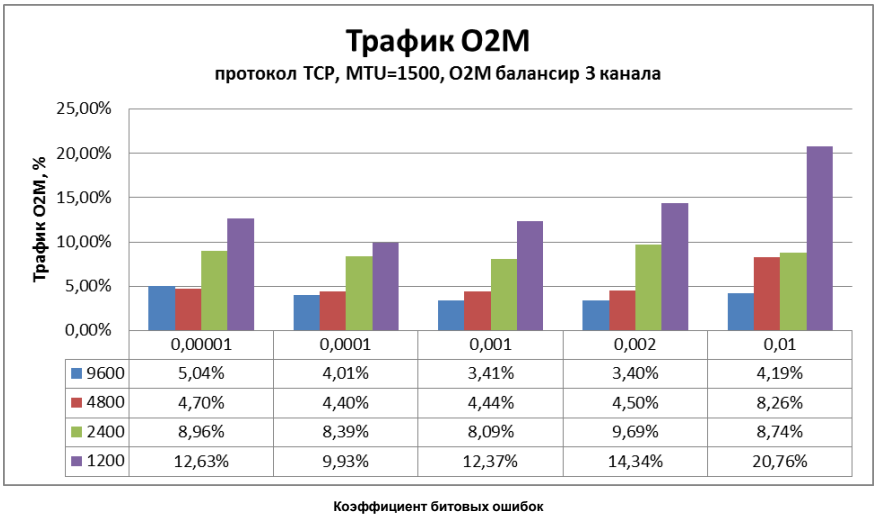


Рис. 3. Структура трафика О2П

Процентное соотношение трафика О2П в общей структуре трафика не зависит от скорости канала, но линейно возрастает в зависимости от КОШ в диапазоне до 10^{-3}. При КОШ 10^{-2} трафик О2П достаточно высокий (80 %), это обусловлено предельной помехоустойчивостью служебных сообщений и сообщений с данными (самые сложные условия адаптации протокола к ошибкам в канале). В результате возникает большое количество повторов сегментов О2П протокола.

Результаты работы протокола динамической маршрутизации О2М

При использовании динамической маршрутизации сходимость сети достигалась на всем измеряемом диапазоне коэффициентов ошибок. При этом уровень трафика был невысоким. Процентное соотношение трафика О2М в структуре общего трафика показано на рис. 4, и в среднем не превышает 15 %.

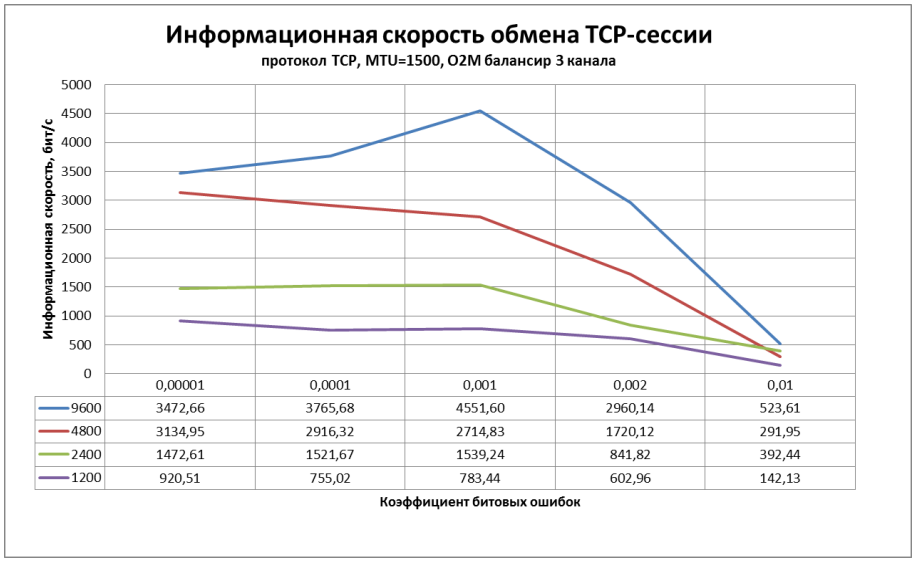


	0,00001	0,0001	0,001	0,002	0,01
9600	5,04%	4,01%	3,41%	3,40%	4,19%
4800	4,70%	4,40%	4,44%	4,50%	8,26%
2400	8,96%	8,39%	8,09%	9,69%	8,74%
1200	12,63%	9,93%	12,37%	14,34%	20,76%

Рис. 4. Структура трафика O2M

Уровень трафика O2M не зависит от коэффициента ошибок, это естественно, так как O2M не имеет сеансового режима обмена – информация об изменении маршрутов проходит широковещательным методом. При уменьшении канальной скорости объем трафика естественно возрастает, так как в данной программной реализации протокола метрическая стоимость канала имеет нелинейную зависимость от скорости передачи, поэтому при низких скоростях изменение метрики происходит чаще, что приводит к более высокому трафику служебных сообщений.

При использовании протокола динамической маршрутизации становится возможным использование режима балансировки нагрузки. В этом режиме маршрут следования *IP*-пакетов может изменяться, в зависимости от загруженности канала и наполненности буферов выдачи пакетов. При этом наблюдается значительное повышение итоговой информационной скорости на каналах с низкой скоростью. Информационная скорость в режиме работы балансира нагрузки при различных КОШ показана на рис. 5.



	0,00001	0,0001	0,001	0,002	0,01
9600	3472,66	3765,68	4551,60	2960,14	523,61
4800	3134,95	2916,32	2714,83	1720,12	291,95
2400	1472,61	1521,67	1539,24	841,82	392,44
1200	920,51	755,02	783,44	602,96	142,13

Рис. 5. Зависимость информационной скорости от КОШ

Прирост информационной скорости при использовании динамической маршрутизации O2П в режиме балансировки нагрузки по 3 каналам показан на рис. 6.

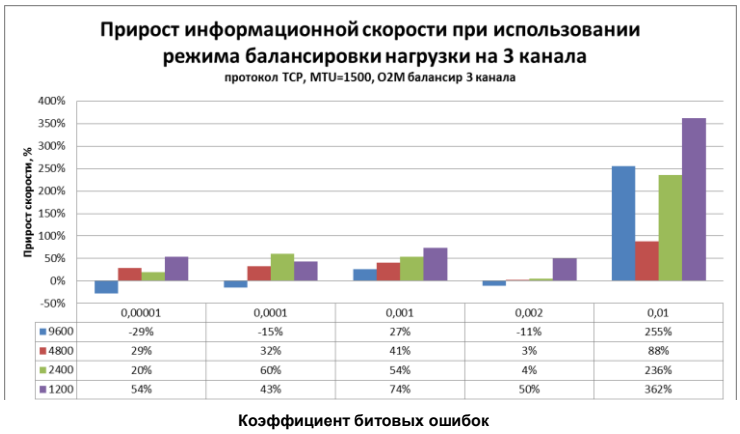


Рис. 6. Прирост информационной скорости при балансировке нагрузки

На гистограмме видно, что при относительном качестве канала (КОШ < 10^{-3}) прирост скорости не превышает 50 %, относительно информационной скорости без использования балансировки нагрузки. Но при низком качестве канала (КОШ 10^{-2}) и низкой скорости 1200 бит/с, прирост в скорости достигает 350 %. Применение режима балансировки нагрузки делает возможным осуществление *TCP*-обмена при низком качестве канала на низких скоростях.

Результаты работы протоколов О2П и О2М в условиях замираний

Особенностью имитируемой динамичной радиосети является возникновение замираний на линиях. Имитация замирания сводится к возникновению непроходимости радиоканала, при котором коэффициент ошибок принимает случайное значение в диапазоне 10^{-2}-10^{0}. Интервал между событиями возникновения замирания на линии характеризуется равномерно распределённой случайной величиной со средним значением 15 минут. Длительность замираний также равномерно распределенная случайная величина со средним значением 5 минут.

При статической маршрутизации такие параметры возникновения замираний являются критическими, в независимости от скорости канала. При ухудшении качества канала на статическом маршруте хуже 10^{-2} всегда наблюдаются разрывы *TCP*-сессии, поэтому провести полноценные испытания и измерения не представляется возможным. В следствие этого, можно сделать вывод, что передача данных по протоколу *TCP* в условиях возникновения замираний и при высоких значениях ошибок в радиоканале в рамках статической маршрутизации невозможна.

При использовании динамической маршрутизации О2М становится возможным вести обмен по протоколу *TCP* в условиях возникновения замираний. График информационной скорости представлен на рис. 7.

Так, при проведении испытаний при скорости канала 1200 бит/с и КОШ не менее 10^{-3} обмен в рамках *TCP*-сессии продолжался более 2 часов без разрывов со средней информационной скоростью 525 бит/с.

При возникновении замирания на линии, метрическая стоимость передачи по данному маршруту резко возрастает. Ухудшение качества канала фиксирует программное обеспечение протокола О2П и передает эту информацию программной реализации протокола О2М. Протокол О2М, в этом случае, должен изменить метрику в базе смежности и отправить широковещательное сообщение. В результате, таблицы маршрутизации перестраиваются, и пакеты следуют по другому маршруту, «обходя» каналы с замиранием. На рис. 8 представлена гистограмма процента служебного трафика О2М в имитируемой сети в условиях возникновения замираний.

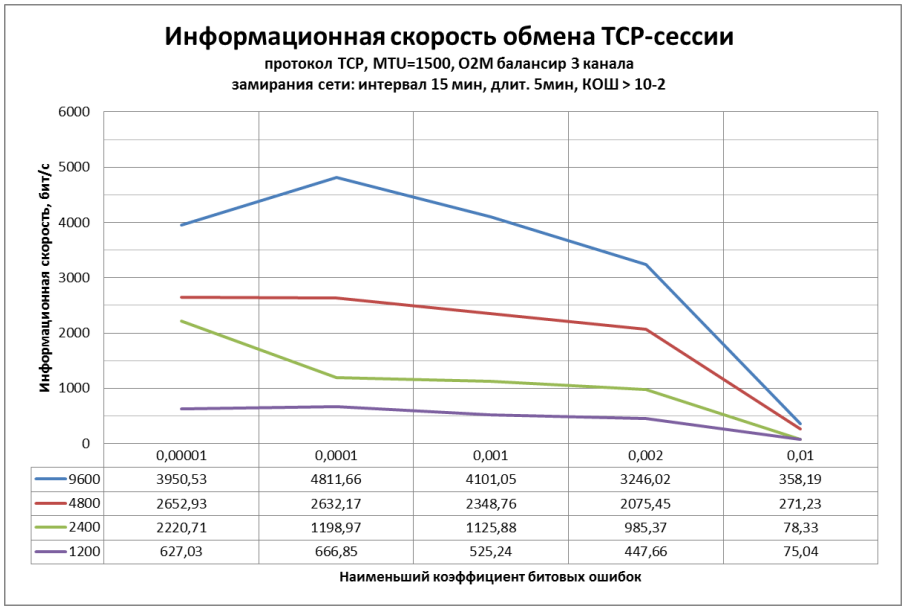


Рис. 7. Информационная скорость при замираниях

Как видно из результатов измерений, процент трафика O2M в общей структуре не зависит от качества (среднего значения коэффициента ошибок) в радиосети. В худшем случае, при средней КОШ 10^{-2} и скорости сети 1200 бит/с трафик O2M занимает 25 % от общего трафика, проходящего по сети. В большинстве случаев, трафик O2M не превышает 10 %.

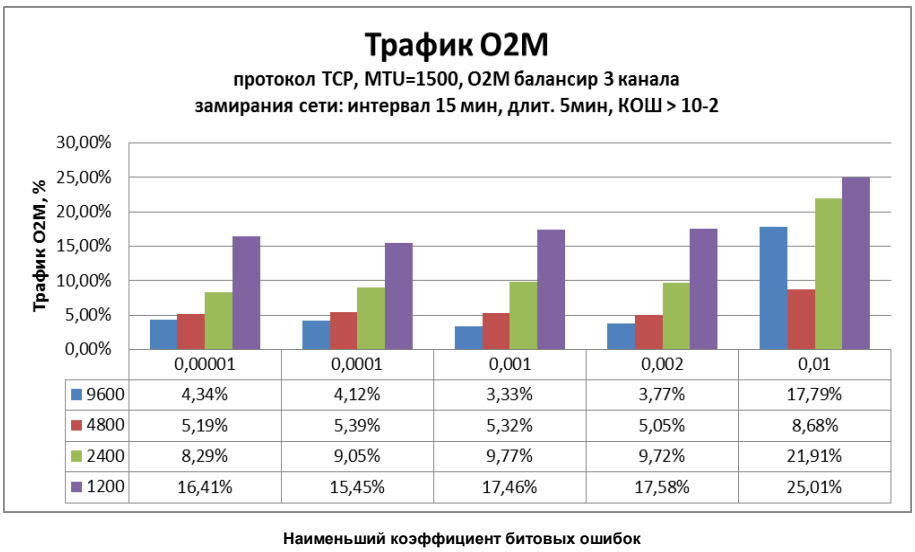


Рис. 8. Структура трафика O2M

Выводы

Результаты испытаний на макете сети из 5 маршрутизаторов показывают, что, благодаря протоколам O2П и O2M, становится возможным передача *IP*-трафика по низкоскоростным сетям с высоким коэффициентом битовых ошибок до 10^{-2}. Протокол динамической маршрутизации O2M позволяет не только формировать таблицы маршрутизации, но и в условиях плохого качества канала осуществлять балансировку трафика, что приводит к повышению пропускной способности. А совместное применение

O2M и O2П позволяет, в прямом смысле, обходить замирания, возникающие в ДКМВ-радиосети.

Недостатком протоколов является требование к наличию полнодуплексной линии, что не всегда возможно в радиосетях. Но этот недостаток вытесняется требованием обеспечения *TCP*-обмена, который в принципе подразумевает двусторонний обмен.

Благодаря встроенному *HDLC*, протоколы O2П/O2M могут работать на низкоскоростных последовательных линиях связи, в том числе и линиях С1И-ФЛ-БИ, а также осуществлять динамическую маршрутизацию в данном сегменте сети.

Отметим, что на приведенном макете, также проверялась возможность работы служб электронной почты и файлового обмена (*FTP*).

В условиях 1200 бит/с и при КОШ 10^{-3} сервера электронной почты, использованные в качестве имитаторов нагрузки успешно обменивались сообщениями. Абоненты данной службы могли обмениваться электронной корреспонденцией с задержками, приемлемыми для данного вида связи.

Проверка работы файлового обмена проводилась с помощью стандартной службы операционной системы (ОС МСВС) по протоколу *FTP*. При указанных условиях, скорость передачи файла, естественно, не превышает канальную скорость, а сама передача занимает достаточное количество времени, но связь стабильная – обрывов сеанса связи не наблюдается, даже при возникновении замираний.

В заключение, хочется отметить, что до недавнего времени возможность передачи *IP*-пакетов по КВ-радиолиниям и интеграция сети КВ-радиосвязи с сетями *TCP/IP* даже не рассматривалась. Подобные сети строились в рамках технологий передачи сообщений и были чрезвычайно специализированы. Применение протоколов O2П и O2M позволит упростить организацию и доступ к радиосети для передачи данных и использовать протокол обмена *TCP/IP*, ставший уже традиционным, для взаимодействия технических средств управления и принятия решений в целях повышения обороноспособности страны и её технологического потенциала.

Литература

1. Ступницкий М.М., Лучин Д.В. Потенциал КВ-радиосвязи – для создания цифровой экосистемы России // Электросвязь. 2018. №5. С. 49-54.

2. Катунин Г.П., Мамчев Г.В., Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 2 – Радиосвязь, радиовещание, телевидение. М.: Горячая линия – Телеком, 2004. 659 с.

3. Головин О.В., Петров С.П. Системы и устройства коротковолновой радиосвязи / Под ред. профессора О.В. Головина. – М.: Горячая линия – Телеком, 2006. 598 с.

4. Меркушев О.В. Процесс определения топологии радиосети передачи данных в декаметровом диапазоне частот // Вестник Удмуртского Университета. Экономика и Право. 2008. №1. С. 139-154.

5. Семенов Ю.А. Протоколы Интернет. Энциклопедия. М.: Горячая линия – Телеком, 2001. 1100 с.

6. Gary R. Wright, W.Richard Stevens TCP/IP Illustrated. Volume 2. The implementation. Addison-Wesly Professional, 1995. 1194 p.

7. Крис Касперски. Могущество кодов Рида-Соломона или Информация, воскресшая из пепла // Системный администратор. 2003. №8. С. 88-94.

References

1. Stupnitsky M.M., Luchin D.V. *Potencial KV-radiosvyazi – dlya sozdaniya cifrovoj ekosistemy Rossii* [Potential of HF radio communication-for creating a digital ecosystem in Russia]. Telecommunication. 2018. No. 5. Pp. 49-54 (in Russian).

2. Katunin G.P., Mamchev G.V., Popantonopulo V.N., Shuvalov V.P. *Telekommunikacionnye sistemy i seti* [Telecommunication systems and networks]. Textbook. In 3 volumes. Volume 2 - Radio communications, Radio broadcasting, Television. Moscow. Hotline-Telecom, 2004. 659 p. (in Russian).

3. Golovin O.V., Petrov S.P. *Sistemy i ustrojstva korotkovolnovoj radiosvyazi* [Systems and devices of short-wave radio communication]. Edited by Professor O.V. Golovin, Moscow. Hotline-Telecom, 2006. 598 p. (in Russian).

4. Merkushev O.V. *Process opredeleniya topologii radioseti peredachi dannyh v dekametrovom diapazone chastot* [The process of determining the topology of the radio data transmission network in the decameter frequency range]. Bulletin Of The Udmurt University. Economics and Law. 2008. №1. Pp. 139-154 (in Russian).

5. Semenov Yu. a. Internet Protocols. Encyclopedia. Moscow. Hotline-Telecom, 2001. 1100 p. (in Russian).

6. Gary R. Wright, W. Richard Stevens TCP/IP Illustrated. Volume 2. The implementation. Addison-Wesly Professional, 1995. 1194 p.

7. Chris Kaspersky. *Mogushchestvo kodov Rida-Solomona ili Informaciya, voskresshaya iz pepla* [The power of Reed-Solomon codes or Information raised from the ashes]. System administrator. 2003. No. 8. Pp. 88-94 (in Russian).

Статья поступила 17 августа 2020 г.

Информация об авторах

Егоров Алексей Александрович – Ведущий инженер-программист отдела разработки функционального программного обеспечения перспективных средств связи ПАО «Интелтех». Тел.: +79022830493. E–mail: EgorovAA@inteltech.ru. Адрес: 197342, г. Санкт-Петербург, Кантемировская ул., д. 8.

O2P and O2M protocols for transferring IP traffic in low-speed networks with a high bit error rate

A.A. Egorov

Annotation. *Proposed O2P and O2M protocols for transmitting TCP/IP traffic and providing dynamic IP-routing in low-speed networks with a high bit error rate, including backbone SW radio networks. The characteristics and modes of operation of protocols are investigated on the network layout in real time. The characteristics of information exchange using developed O2P and O2M protocols in the communication channel with different bit error rate are given.*

Keywords*: Protocol O2P; Protocol O2M; data transmission; dynamic routing; bit error rate; low-speed network; SW; radio communication; TCP Protocol; IP Protocol.*

Information about Authors

A.A. Egorov – Leading software engineer of the Department of functional software development for advanced communications, PJSC IntelTech. Tel.: +79022830493. E–mail: EgorovAA@inteltech.ru. Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya street, 8.

Для цитирования: Егоров А.А. Протоколы О2П и О2М для переноса IP-трафика в низкоскоростных сетях с высоким коэффициентом ошибок // Техника средств связи. 2020. № 3 (151). С. 19-28.

For citation: Egorov A.A. O2P and O2M protocols for transferring IP traffic in low-speed networks with a high bit error rate. Means of communication equipment. 2020. No 3 (151). Pp. 19-28 (in Russian).

УДК 621.396

Импульсное регулирование в преобразователях постоянного тока системы автономного электроснабжения комплексов связи

Абрамкин Р.В., Веселовский А.П., Виноградено А.М., Крачков А.А.

Аннотация: *в статье рассматривается наиболее динамично развивающееся направление силовой электроники, связанное с решением задачи регулирования напряжения в преобразователях постоянного напряжения. Проведен анализ работы преобразователей напряжения. Показана возможность получения полной линейной регулировочной характеристики, используя широтно-импульсный метод. Представлен способ линейного регулирования выходного напряжения с помощью широтно-импульсной модуляции.*

Ключевые слова: *регулирование напряжения; статические преобразователи энергии; система автономного электроснабжения; широтно-импульсное модулирование.*

Введение

В настоящее время техника связи представляет собой изделия принципиально нового уровня информатизации и интеллектуализации. Использование таких устройств позволяет существенно расширить функционал системы связи, однако их техническая сложность влечет за собой повышенные требования к вторичным источникам питания, входящим в состав системы автономного электроснабжения комплексов связи (САЭКС).

САЭКС представляет собой совокупность технических средств, предназначенных для обеспечения потребителей электрической энергией заданного качества в необходимом количестве в районе выполнения задачи.

В состав современных САЭКС входят электромеханические источники электроэнергии, а также значительное количество вторичных источников питания, представляющих собой системообразующее электротехническое оборудование.

Одними из наиболее значимых элементов данного оборудования являются импульсные преобразователи постоянного тока, так как во многом их работа определяет состояние системы, в целом. Они требуют повышенной точности и скорости регулирования в разомкнутых и замкнутых системах управления. Использование энергосберегающего регулируемого преобразователя постоянного тока позволяет улучшить эксплуатационные характеристики САЭКС, в целом.

Основным параметром преобразователя, наиболее остро влияющим на работу САЭКС, является регулировочная характеристика, степень линейности которой определяет точность и скорость регулирования [1-15].

Принципы преобразования постоянного напряжения

Выпускаемые промышленностью современные преобразователи включают в себя: пульт местного и дистанционного управления, буквенно-цифровые индикаторы отображения информации о входном и выходном напряжениях, выходном токе, частоте, точности поддержания различных параметров и других данных [5-13].

Для улучшения потребительских свойств изделий оптимизируют параметры, повышают рабочую частоту преобразования, уменьшают потери мощности на силовых элементах, а также снижают динамические нагрузки в силовой части схемы. Для регулирования переменного и постоянного напряжений используются широтно-импульсные методы модулирования с изменением скважности импульсов [5].

Широтно-импульсные преобразователи постоянного напряжения преобразуют постоянное напряжение в импульсное, среднее значение которого (т. е. его постоянную составляющую, выделяемую в нагрузке фильтрами) можно регулировать. Выходное

напряжение таких преобразователей (до выходного фильтра), как правило, имеет вид однополярных импульсов.

Частота дискретизации зависит от динамических свойств вентилей, на которых выполнен преобразователь. В связи с постоянным напряжением, на входе преобразователя естественная коммутация вентилей невозможна, что требует его исполнения на вентилях с полным управлением (запираемые тиристоры, транзисторы). *GTO*-тиристоры допускают переключения до 1 кГц, *IGBT*-транзисторы – примерно до 10 кГц, полевые транзисторы – до 1 МГц и выше. Очевидно, что частота коммутации определяет возможную скорость регулирования параметров преобразованной энергии и габариты реактивных элементов.

Регулировочная характеристика широтно-импульсного преобразователя постоянного напряжения – зависимость относительного среднего значения его выходного напряжения (в долях среднего значения входного) от относительной длительности импульса напряжения на выходе. Эта длительность импульса напряжения определяется по отношению к периоду следования импульсов.

Уравнение регулировочной характеристики широтно-импульсного преобразователя с однополярными импульсами (однополярная модуляция), определяющее степень регулирования выходного напряжения, имеет вид:

$$C = \frac{U\text{вых}}{U\text{вх}} = \frac{1}{TU\text{вх}} \int_0^{tu} U\text{вх}dt = \frac{tu}{T}.$$

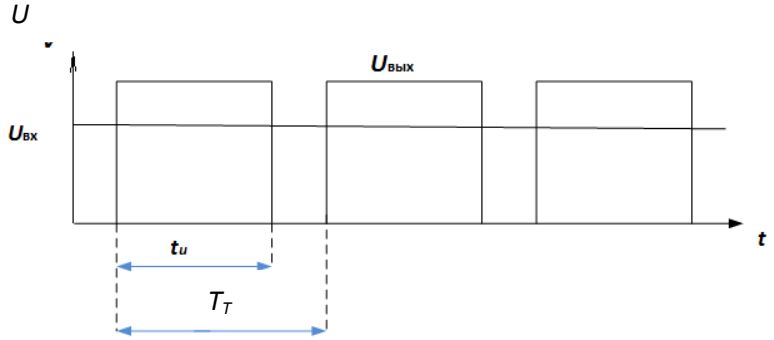


Рис. 1. Выходное напряжение преобразователей с однополярными импульсами

Существенным моментом в преобразователях постоянного тока является желаемая линейная зависимость выходного напряжения от управляющего воздействия. Особенностью зависимости $U_{\text{вых}} = f(U_{\text{упр}})$ при широтно-импульсной модуляции (ШИМ) напряжения является нелинейность выходной характеристики [1]. Регулировочная характеристика при таком способе регулирования имеет круто падающий характер.

Разработан способ получения линейной регулировочной характеристики с помощью широтно-импульсного метода управления силовыми элементами преобразователя [1].

Частичное линейное регулирование постоянного напряжения возможно, используя метод широтно-импульсного модулирования при изменении угла управления α по арккосинусоидальному закону [1]. Линейность характеристики является большим достоинством преобразователя, обеспечивающим оптимальное построение устройств автоматического управления процессами в выходной цепи выпрямителей. В настоящий момент существует метод регулирования выходного напряжения с ШИМ, который позволяет получить линейную регулировочную характеристику в пределах $0,56U_{\text{вх}}$. Подобный подход был предложен для инверторов (регулирование переменного напряжения), где амплитуда синусоиды не превышает амплитуду треугольных импульсов.

Наибольшее применение на практике получили три способа широтно-импульсного регулирования:

1) Регулирование по закону, когда среднее значение выходного напряжения и ширина изменяются по прямоугольному признаку.

2) Регулирование по трапецеидальному закону – в этом случае среднее значение выходного напряжения имеет вид трапеции.

3) Регулирование по синусоидальному закону, когда ширина импульсов выходного напряжения регулируется по синусоидальному закону.

В основу устройств широтно-импульсного регулирования однофазных и трехфазных инверторов напряжения положен нуль-орган (компаратор), на неинвертирующий вход которого подается опорное ($U_{оп}$) напряжение треугольной формы, а на инвертирующий – модулирующее напряжение $U_{м}$ прямоугольной, трапецеидальной или синусоидальной формы.

На рис. 2 показан принцип формирования модулирующих импульсов с помощью нуль-органа при модулирующем напряжении $U_{м}$ прямоугольной формы и опорном напряжении треугольной формы $U_{оп}$: а) нуль-орган (компаратор); б) кривые опорного и модулирующего напряжений; в) кривые выходного напряжения нуль-органа.

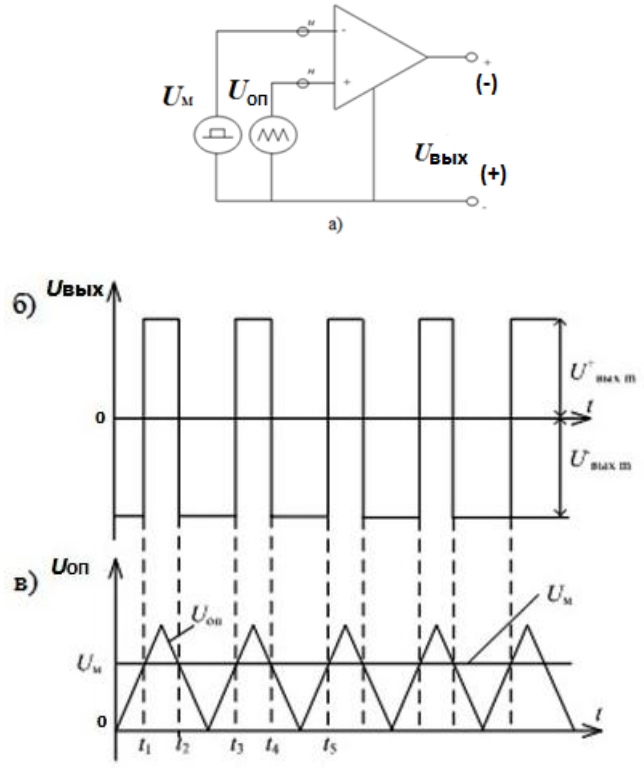


Рис. 2. Формирователь модулирующих импульсов

В точках равенства опорного и модулирующего напряжений в моменты времени t_1, t_2, t_3, t_4 происходит срабатывание компаратора. В результате, на выходе формируются импульсы напряжений, длительность которых изменяется пропорционально модулирующему напряжению. Отсюда, данный способ получил название широтно-импульсного модулирования (ШИМ).

В промежутках времени $0-t_1, t_2-t_3$ значение $U_{оп} < U_{м}$, в результате чего на выходе формируются отрицательные импульсы выходного напряжения.

В промежутках времени $t_1 - t_2, t_3 - t_4, U_{оп} > U_м$, что приводит к изменению полярности выходных импульсов напряжения. Изменяя величину постоянного модулирующего напряжения, можно регулировать ширину положительных и отрицательных импульсов выходного напряжения компаратора. Полученные импульсы напряжения позволяют с помощью программируемых контроллеров сформировать импульсы управления транзисторами инверторов по заданному закону.

Принципиально, в однофазных инверторах формирование импульсов напряжения может быть выполнено при однополярном опорном напряжении треугольной формы и двуполярном – пилообразной формы. В трехфазных инверторах система управления ШИМ может быть выполнена только при двуполярном опорном напряжении.

Авторами предложен метод регулирования выходного напряжения с ШИМ, который позволяет получить линейную регулировочную характеристику постоянного напряжения в диапазоне регулирования от 0 до 1 [13].

Особенности регулирования напряжения методом ШИМ

Реализация метода ШИМ осуществляется на основе представленного на рис. 3-6 принципа.

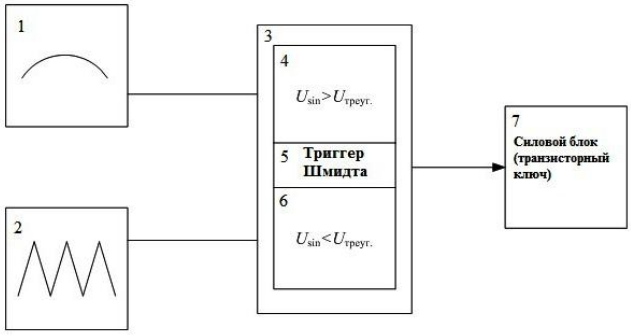


Рис. 3. Схема реализации метода ШИМ

Схема управления содержит генератор положительных полуволн синусоидального напряжения (1) и треугольных импульсов (2), блок формирования управляющего сигнала (3), состоящий из блоков сравнения опорного и модулирующего напряжений (4) и (6), триггера Шмидта (5) и силового блока (7).

На рис. 4-6 показан принцип формирования управляющих импульсов при помощи схемы, представленной на рис. 3.

ШИМ осуществляется следующим образом: положительная полуволна синусоидального сигнала управления пересекает треугольные импульсы в диапазоне 0 … π. Регулируемое напряжение постоянного тока (для силовой части схемы) разбивается на прямоугольные импульсы, в соответствии с условием пересечения треугольных импульсов с синусоидальной кривой. Получаем девять импульсов различной длительности.

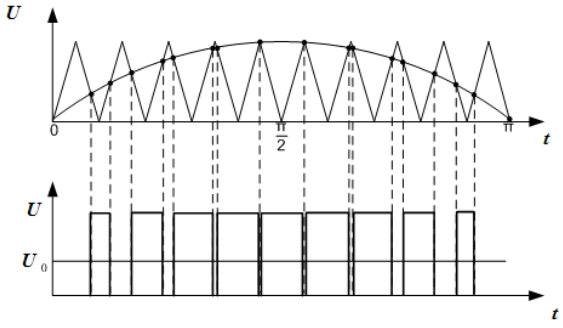


Рис. 4. Регулирование выходного напряжения ШИМ для постоянного напряжения ($U_{sin} > U_{треуг}$)

Таким образом, постоянное напряжение разбивается на ряд участков с наличием или отсутствием напряжения. При этом, модулированное напряжение будет присутствовать в диапазонах, где значение напряжения синусоидальной формы превышает значение напряжения треугольных импульсов (рис. 4). Среднее значение напряжения на нагрузке будет определяться длительностью и частотой прямоугольных импульсов, т. е. их скважностью. Изменение скважности, а равно и регулирование напряжения на выходе преобразователя (U_0), достигается изменением амплитуды положительной полуволны синусоидального напряжения (рис. 5).

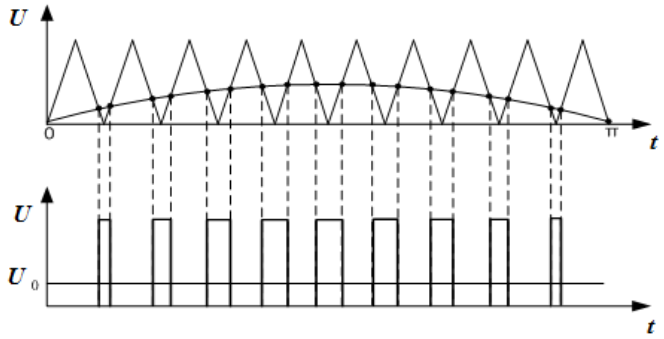


Рис. 5. Изменение скважности импульсов путем изменения амплитуды положительной полуволны синусоидального сигнала

Не смотря на полученную линейность регулировочной характеристики, при таком способе регулирования напряжения U_0 на выходе преобразователя, диапазон регулирования составляет чуть более половины от входного значения напряжения.

С целью осуществления возможности регулирования выходного напряжения U_0 от 0 до 1, применяются способ, представленный на рис. 6.

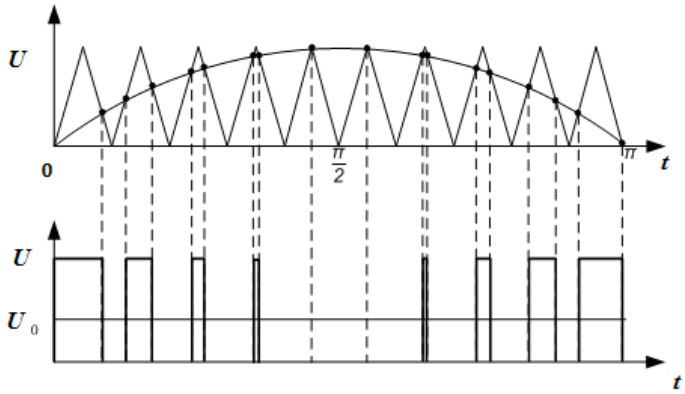


Рис. 6. Регулирование выходного напряжения ШИМ для постоянного напряжения ($U_{\text{sin}} < U_{\text{треуг}}$)

Формирование прямоугольных импульсов происходит в моменты, когда амплитуда напряжения треугольных импульсов превышает значение синусоиды ($U_{\text{sin}} < U_{\text{треуг}}$).

Регулирование выходного напряжения U_0 также достигается изменением амплитуды синусоиды.

Регулировочная характеристика, полученная в результате применения настоящего способа регулирования напряжения, будет иметь вид, представленный на рис. 7.

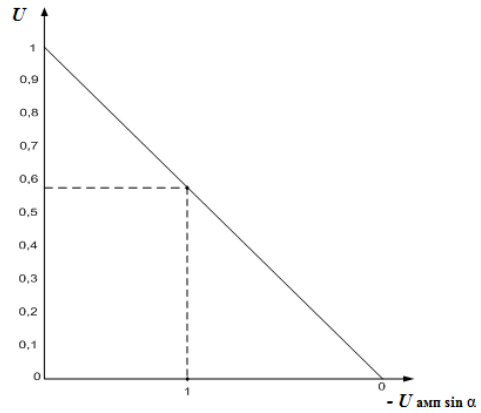


Рис. 7. Регулировочная характеристика преобразователя постоянного тока в диапазоне регулирования от 0 до 1

Основное достоинство ШИМ связано с отсутствием в нем каких-либо реактивных элементов (дросселей, конденсаторов), что позволяет выполнять его в едином технологическом процессе в виде твердотельного модуля. Это обеспечивает низкие удельные значения массогабаритных показателей преобразователя. Недостатки же связаны с импульсным характером токов и напряжений, что обуславливает высокие уровни помех и низкий уровень электромагнитной совместимости.

Заключение

В результате применения метода ШИМ, регулировочные характеристики постоянного напряжения имеют линейный характер и позволяют производить регулирование напряжения от нулевых значений до максимальных. При этом, значительно упрощается использование микропроцессорной техники для изготовления регуляторов напряжения. Результаты по разработанному алгоритму работы управляющего устройства методом ШИМ могут найти широкое применение в силовой электронике САЭКС.

Дальнейшими направлениями совершенствования САЭКС являются ориентация на разработку способов преобразования электроэнергии, а также улучшение эксплуатационно-технических характеристик вторичных источников электропитания, стабильная работа которых определяет стабильность работы системы связи, в целом.

Литература

1. Семенов Б.Ю. Силовая электроника: профессиональные решения. М.: Солон-пресс. 2011. 416 с.

2. Розанов Ю.Г. Основы силовой электроники. М.: Энергоатомиздат, 1992. 296 с.

3. Соколовский Г.Г. Электроприводы переменного тока с частотным регулированием. М.: ACADEMA. 2006. 265 с.

4. Роташ Э.М., Дробович Ю.И., Юрченко Н.Н., Шевченко П.Н. Высокочастотные транзисторные преобразователи. М.: Радио и связь. 1988.

5. Веселовский А.П., Будко П.А., Бурьянов О.Н., Виноградено А.М. Особенности систем управления вентильных преобразователей // Тезисы докладов II межвузовской НПК «Проблемы технического обеспечения войск в современных условиях» ВАС; СПб, 2017 г., с. 150-154.

6. Веселовский А.П., Будко П.А., Виноградено А.М., Косарева Л.И. Реализация способа преобразования переменного напряжения // Тезисы докладов II межвузовской НПК «Проблемы технического обеспечения войск в современных условиях» ВАС; СПб, 2018 г., с. 172-176.

7. Веселовский А.П., Будко П.А., Виноградeнко А.М., Косарева Л.И. Регулирование напряжения в преобразователях высокочастотными импульсами с изменяющейся скважностью // Мехатроника, автоматизация, управление. 2018. №8 (19). С. 516-522. DOI: 10.17587/mau. 19.516-522.

8. Виноградeнко А.М., Веселовский А.П., Вжесневский С.В., Гальвас А.В. Способ и устройство синхронизации систем управления преобразователей напряжения // Практическая силовая электроника. 2018. № 2 (70). С. 53-55.

9. Гельман М.В., Гельман М.М., Преображенский К.А. Преобразовательная техника. Челябинск. ЮУрГУ. 2009. 425 с.

10. Кулик В.Д. Силовая электроника. Автономные инверторы, активные преобразователи: Учебное пособие. СПб.: СПбГТУРП, 2010. 90 с.

11. Зиновьев Г.С. Силовая электроника. Учебн. пособие для бакалавров. Москва: Юрайт. 2012. 671с.

12. Abraham L., Heumann K., Koppelmann F. Wechselrichter fur Dzehzahlsteurung von Kafiglaufermotoren. AEG–Mitt., 1964. N. 2. P. 89-106.

13. Volkov A.G. Mathematical model of AC-AC converter without passive elements in DC-link // Source of the Document International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM 2014). 2014. P. 403-407.

References

1. Semenov B.Yu. Power electronics: professional solutions. Moscow. Solon-press. 2011. 416 p. (in Russian).

2. Rozanov Yu.G. Fundamentals of power electronics. Moscow. Energoatomizdat, 1992. 296 p. (in Russian).

3. Sokolovsky G.G. *Elektroprivody peremennogo toka s chastotnym regulirovaniem* [Electric drives of alternating current with frequency regulation]. Moscow. Academa. 2006. 265 p. (in Russian).

4. Rotash E.M., Drobovich Yu.I., Yurchenko N.N., Shevchenko P.N. *Vysokochastotnye tranzistornye preobrazovateli* [High-Frequency transistor converters. Moscow. Radio and communications]. 1988 (in Russian).

5. Veselovsky A.P., Budko P.A., On Weeds.N., and Vinogradenko.M. *Osobennosti sistem upravleniya ventil'nyh preobrazovatelej* [Features of control systems valve converters]. Proceedings of the second Intercollegiate NPK "problems of technical support of troops in modern conditions". Saint-Petersburg. 2017 p. 150-154 (in Russian).

6. Veselovsky A.P., Budko P.A., Vinogradenko And.M. Kosareva L.I. *Realizaciya sposoba preobrazovaniya peremennogo napryazheniya* [The Implementation of the method of conversion of alternating voltage]. Abstracts of the second inter-University SPC "problems of technical support of troops in modern conditions". Saint-Petersburg 2018 p. 172-176 (in Russian).

7. Veselovsky A.P., Budko P.A., Vinogradenko a.m., Kosareva L.I. *Regulirovanie napryazheniya v preobrazovatelyah vysokochastotnymi impul'sami s izmenyayushchejsya skvazhnost'yu* [Voltage Regulation in converters by high-frequency pulses with varying duty cycle]. Mechatronics, automation, and control. 2018. No. 8 (19). Pp. 516-522. DOI: 10.17587/mau. 19. p. 516-522 (in Russian).

8. Vinogradenko A.M., Veselovsky A.P., Vzhesnevsky S.V., Galvas A.V. *Sposob i ustrojstvo sinhronizacii sistem upravleniya preobrazovatelej napryazheniya* [Method and device for synchronizing control systems of voltage converters]. Practical power electronics. 2018. No. 2 (70). Pp. 53-55 (in Russian).

9. Gelman M.V., Gelman M.M., Preobrazhensky K.A. Transformative technology. Chelyabinsk. SUSU. 2009. 425 p. (in Russian).

10. Kulik V.D. Power electronics. Stand-alone inverters, active converters. Saint Petersburg, 2010, 91 p. (in Russian).

11. Zinoviev G.S. Power electronics. Moscow: Yurayt. 2012. 671 s. (in Russian).

12. Abraham L., Heumann K., Koppelman, F. von Wechselrichter fur Dzehzahlsteurung Kafiglaufermotoren. AEG–Mitt., 1964. N. 2. P. 89-106.

13. Volkov A.G. mathematical model of frequency Converter AC to AC without passive elements in DC link. Source document of the International conference of young specialists on micro/nanotechnologies and electron devices (EDM 2014). 2014. Pp. 403-407.

Статья поступила 28 августа 2020 г.

Информация об авторах

Абрамкин Роман Викторович – Адъюнкт кафедры Технического обеспечения связи и автоматизации Военной академии связи. Тел. +7-999-980-85-13. E-mail: avg62rus@rambler.ru.

Веселовский Анатолий Платонович – Кандидат технических наук, доцент института электропитания СПбГПУ. Тел. +7-904-559-48-44. E-mail: aveselovskij@mail.ru.

Виноградeнко Алексей Михайлович – Кандидат технических наук, доцент, докторант кафедры Технического обеспечения связи и автоматизации Военной академии связи. Тел. +7-921-443-90-22. E-mail: vinogradenko.a@inbox.ru.

Крачков Андрей Александрович – Адъюнкт кафедры Технического обеспечения связи и автоматизации Военной академии связи. Тел. +7-938-863-51-73. E-mail: kr.andrew@mail.ru.

Адрес: 194064, Россия, Санкт-Петербург, Тихорецкий пр., д.3.

Pulse regulation in dc converters of autonomous power supply systems for communication complexes

R.V. Abramkin, A.P. Veselovsky, A.M. Vinogradenko, A.A. Krackow

Abstract: *the article deals with the most dynamically developing direction of power electronics associated with the solution of the problem of voltage regulation in DC converters the analysis of the work of voltage converters. The possibility of obtaining a complete linear adjustment characteristic using the pulse-width modulation is presented.*

Keywords: *voltage regulation; static energy converters;independent power supply system; pulse-width modulate.*

Information about Authors

Abramkin Roman Viktorovich – Associate of the Department of Technical Support of Communications and Automation of the Military Academy of Communications. Tel. +7-999-980-85-13. E-mail: avg62rus@rambler.ru.

Veselovsky Anatoly Platonovich – Candidate of technical sciences, associate professor of the power supply institute of St. Petersburg State Pedagogical University. Tel. +7-904-559-48-44. E-mail: aveselovskij@mail.ru.

Vinogradenko Alexey Mikhailovich – Ph.D., associate professor, doctoral student of the Department of Technical Support of Communications and Automation of the Military Academy of Communications. Tel. +7-921-443-90-22. E-mail: vinogradenko.a@inbox.ru.

Krachkov Andrey Alexandrovich – Associate Professor of the Department of Technical Support of Communications and Automation of the Military Academy of Communications. Tel. +7-938-863-51-73. E-mail: kr.andrew@mail.ru.

Address: 194064, Russia, Saint-Petersburg, Tikchoretskiy pr., d. 3.

Для цитирования: Абрамкин Р.В., Веселовский А.П., Виноградeнко А.М., Крачков А.А. Импульсное регулирование в преобразователях постоянного тока системы автономного электроснабжения комплексов связи // Техника средств связи. 2020. № 3 (151). С. 29-36.

For citation: Abramkin R.V., Veselovsky A.P., Vinogradenko A.M., Krackow A.A.Pulse regulation in dc converters of autonomous power supply systems for communication complexes. Means of communication equipment. 2020. No 3 (151). Pp. 29-36 (in Russian).

ПЕРЕДАЧА, ПРИЕМ И ОБРАБОТКА СИГНАЛОВ

УДК 621.396.4, 519.876.5

Использование сигнально-кодовой конструкции аппаратуры передачи данных для сравнения моделей радиоканала

Шаптала В.С., Машкин А.И., Соколов В.А.

Аннотация. *В статье ставится задача сопоставить результаты определения помехоустойчивости многоканального пакетного модема, полученные двумя способами: с использованием встроенных функций системы технических расчетов MATLAB и с использованием модели канала из прототипа опытного района цифровой сети радиосвязи. Целью работы является получение кривых помехоустойчивости для основных типов состояния радиоканала в соответствии с рекомендацией ITU-R F-1487. При моделировании используются методы кроссплатформенного программирования и цифровой обработки сигналов. Новизна обсуждаемого решения состоит в сопоставлении двух моделей радиоканала, выполненных в соответствии с рекомендацией ITU-R F-1487. К результатам работы следует отнести графики помехоустойчивости разрабатываемого модема. Практическая значимость исследования заключается в возможности демонстрации функционирования модема без проведения трассовых испытаний и возможности сравнения модемов различных исполнителей в лабораторных условиях.*

Ключевые слова: *помехоустойчивость; сигнально-кодовые конструкции; цифровая обработка сигналов; коротковолновый диапазон частот.*

Введение

Проверка помехоустойчивости сигнально-кодовой конструкции часто является сложной задачей, поскольку требует проведения дорогостоящих и длительных трассовых испытаний. Регламент проведения подобного рода экспериментов требует получения набора частот, которые можно легитимно использовать. Этот набор частот выдается на определенное время, что усложняет организацию испытаний и не допускает проведение предварительных проверок. Особенно сложно организовать трассовые испытания для удаленных абонентов, поскольку это часто требует необходимости создания канала служебной связи для управления испытаниями, и для каналов с изменяющимися во времени характеристиками. Все вышесказанное ярко проявляется при разработке аппаратуры передачи данных (АПД) в коротковолновом (КВ) диапазоне частот:

– расстояние между абонентами от 3000 км и больше;

– абоненты расположены в труднодоступных районах;

– параметры КВ канала изменяются с течением времени.

Проводя в таких условиях трассовые испытания, очень тяжело сопоставить результаты, поскольку трудно добиться повторяемости экспериментов, поэтому Международный союз электросвязи настоятельно рекомендует использовать для тестирования сигнально-кодовых конструкций модели каналов и проводить вычислительные эксперименты в лабораторных условиях. Для КВ диапазона необходимо использовать рекомендацию *F*.1487 [1] 2000 г., которая заменяет рекомендацию *F*.520 [2] 1992 г.

При использовании моделей канала всегда возникает вопрос о том, насколько точно они соответствуют рекомендации *F*.1487, поскольку официальных способов их сертификации, с точки зрения авторов, не существует. Часто эти модели создаются на целевой элементной базе с поддержкой специфического набора интерфейсов, поскольку целесообразно создавать модель, похожую на используемые радиосредства, поэтому и возникает необходимость сопоставить работу своей модели канала и выбранной общеизвестной. В статье рассматриваются две модели канала: одна из системы технических

расчетов *MATLAB*, а другая из состава распределенной модели опытного района цифровой сети радиосвязи [3].

Виды радиоканалов из рекомендации *ITU-R F*.1487

Рекомендация F.1487 описывает 10 состояний ионосферных каналов. Каждый канал характеризуется задержкой между лучами (*differential time delay*) и расширением спектра в каждом луче (*doppler spread*), как представлено в табл.

Таблица – Характеристика задержек между лучами и расширением спектра в каждом луче

Ионосферные каналы, определенные рекомендацией *ITU-R F*.1487	Задержка, мс	Расширение спектра, Гц
Low latitudes, Quiet conditions	0.5	0.5
Low latitudes, Moderate conditions (*Poor Channel*)	2	1.5
Low latitudes, Disturbed conditions	6	10
Mid-latitudes, Quiet conditions (*Good Channel*)	0.5	0.1
Mid-latitudes, Moderate conditions (*Moderate Channel*)	1	0.5
Mid-latitudes, Disturbed conditions	2	1
Mid-latitudes, Disturbed near vertical incidence	7	1
High latitudes, Quiet conditions	1	0.5
High latitudes, Moderate conditions	3	10
High latitudes, Disturbed conditions	7	30

Для проведения моделирования работы модема в условиях замираний и построения графиков помехоустойчивости были выбраны три типа канала: *Good*, *Moderate* и *Poor Channel*. Выбор только этих каналов обусловлен историческим фактором (они появились в рекомендации *F*.520) и желанием уменьшить время на проведение тестирования.

Особенности определения мощности шума в модели канала

Для корректного добавления аддитивного шума к сигналу необходимо получить выражение для его мощности. Для этого рассмотрим отношение сигнал/шум по мощности – *SNR*.

Из теории связи, например [4], известно, что:

$$SNR = \frac{P_s}{P_n} = \frac{P_s}{N_0 W},$$

где P_S – мощность сигнала, P_n – мощность шума, N_O – спектральная плотность мощности (СПМ) белого шума, W – ширина спектра сигнала.

Для сопоставления различных схем модуляции и кодирования сигнала используется другая мера отношения сигнал/шум – отношение сигнал/шум на бит, которое определяется как отношение энергии сигнала на один бит передаваемых данных, к спектральной плотности мощености (СПМ) белого шума – E_b/N_o дБ.

Для того, чтобы установить связь между двумя этими метриками необходимо заметить, что мощность сигнала равна энергии бита, умноженной на битовую скорость – R бит/с: $P_s = E_b R$. С учетом этого из (1) получаем:

$$SNR = \frac{E_b R}{N_0 W} = \frac{E_b}{N_0}\left(\frac{R}{W}\right).$$

Связь битовой скорости с символьной определяется следующим образом:

$$R_s = \frac{R}{m} = \frac{1}{T_s} = f_s,$$

где R_S – символьная скорость символ/с, m – количество бит на символ, T_S – длительность передачи символа, fs – частота передачи символа.

Учитывая, что полоса комплексного сигнала в канале с аддитивным белым гауссовским шумом (АБГШ, *AWGN*) ограничена частотой дискретизации ($W = f_d$), вместе с (3) из выражения (2) получаем:

$$SNR = \frac{E_b}{N_o}\left(\frac{mR_s}{W}\right) = \frac{E_b}{N_o}\left(\frac{mf_s}{f_d}\right).$$

Или в более привычной логарифмической форме:

$$SNR = \frac{E_b}{N_o} + 10\lg(m) + 10\lg\left(\frac{f_s}{f_d}\right).$$

Полученная формула (5), позволяет задать необходимое значение *SNR* с учетом полосы сигнала и кратности модуляции.

Таким образом, с учетом (1) и (5), получаем формулу для оценки мощности шума:

$$P_n = P_s - \frac{E_b}{N_o} - 10\lg(m) - 10\lg\left(\frac{f_s}{f_d}\right).$$

Еще одной полезной метрикой для сравнения различных схем модуляции с учетом их позиционности является метрика отношения энергии символа E_s к СПМ белого шума – E_s/N_o дБ. Для установления связи между E_s/N_o и E_b/N_o необходимо воспользоваться следующим соотношением: $E_s = P_s T_s = P_s m/R = mE_b$. Таким образом, выражение для отношения сигнал/шум на символ принимает вид:

$$\frac{E_s}{N_o} = \frac{E_b}{N_o} + 10\lg(m).$$

Особенности реализации модели канала в среде *MATLAB*

Каналы, в соответствии с рекомендацией *F*.1487, реализованы в пакете *communication toolbox* из системы технических расчетов *MATLAB.*

Для установки параметров канала используется встроенная функция – *stdchan (chnatype, r_s, f_d)*, которая возвращает объект в соответствии с указанным типом канала – *chnatype*, частотой дискретизации – r_s и максимальным доплеровским сдвигом – f_d. Параметр *chnatype* выбирается из моделей каналов, перечисленных в стандарте, частота дискретизации *rs* соответствует частоте дискретизации сигнала, параметр f_d для каналов из рекомендации *F*.1487 должен составлять значение 1 Гц.

Реализацию искажений в рэлевском и АБГШ канале берут на себя классы: *comm.RayleighChannel* и *comm.AWGNChannel*. В качестве аргументов класс *comm.RayleighChannel* принимает результат функции *stdchan*, а класс *comm.AWGNChannel* позволяет устанавливать отношение сигнал/шум различными способами.

Описание эксперимента

Моделирование проводилось с помощью приложений *fhss-standalone* и *fhss-fileusage.* Отличительной особенностью данных приложений является то, что *fhss-standalone* использует свою, разработанную на языке программирования Си, модель канала с замираниями, тогда как *fhss-fileusage*, позволяет использовать внешнюю модель канала, в нашем случае, из среды *MATLAB.*

Структурная схема эксперимента приведена на рис. 1. Цель эксперимента заключалась в определении коэффициента битовой ошибки (*BER, Bit Error Rate*) для АБГШ канала и трех выбранных каналов из рекомендации *F*.1487.

Модель КВ канала состоит из рэлеевского двухлучевого канала и канала с АБГШ. При работе с *fhss-fileusage* модулированные сигналы были записаны в бинарные файлы,

которые считывались в среде *MATLAB*, искажались в соответствии с моделью КВ канала и записывались в бинарный файл. Искаженные таким образом сигналы, демодулировались приложением *fhss-fileusage* в котором происходил расчёт вероятности ошибки. В случае с *fhss-standalone*: модуляция, искажения, демодуляция и оценка *BER* происходили непрерывно в одном приложении.

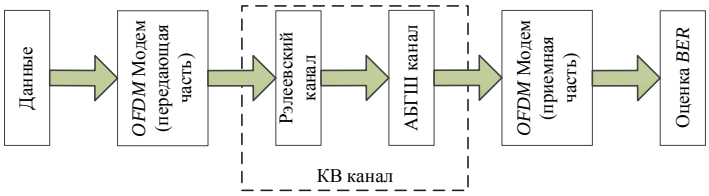


Рис. 1. Структурная схема эксперимента

Результаты моделирования

Параметры *OFDM* модема: ОФМ – 2, 4, 8; количество информационных поднесущих – 44; интервал ортогональности – 10 мс; защитный интервал – 2,5 мс; длительность слота T – 50 мс; количество посылок в слоте – 4; помехоустойчивый код для соответствующих позиционностей модуляции – код Рида-Соломона (26,16), (44,24), (33,23); информационная скорость 1600, 2880, 5440 бит/с.

Количество информационных поднесущих в модеме – 44, расстояние между ними обратно интервалу ортогональности и составляет 100 Гц, следовательно – fs = 4400 Гц, частота дискретизации f_d = 12800 Гц, кратность модуляции m = 1, 2, 3.

Количество передаваемых информационных бит во всех экспериментах было не менее 10^6. Диапазон отношения сигнал/шум для экспериментов: в АБГШ канале – от 0 до 20 дБ с шагом 1 дБ, в каналах с замираниями – от 0 до 30 дБ с шагом 2 дБ. Одни и те же кривые *BER*, для удобства анализа, построены для различных определений отношения сигнал/шум: E_b/N_o, E_s/N_o и *SNR*. Результаты экспериментов представлены на рис. 2-4 в диапазоне от 0 до 20 дБ, поскольку в статье рассматриваются только низкоскоростные модемы, которые должны функционировать при малых отношениях сигнал/шум.

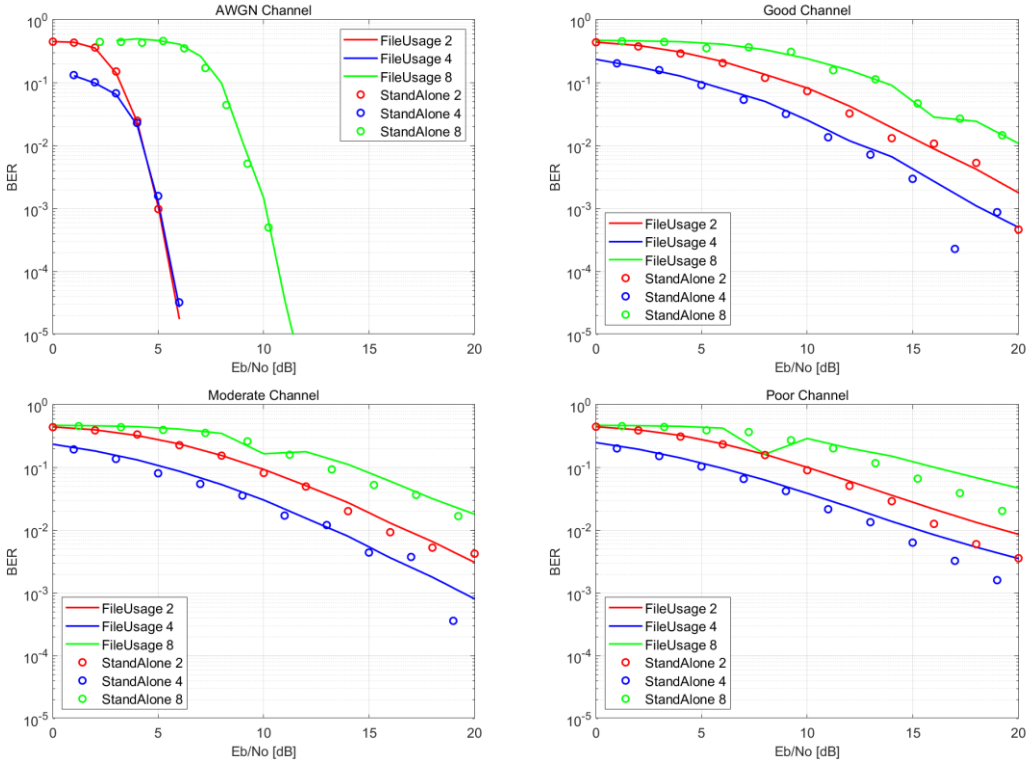


Рис. 2. *BER* в зависимости от E_b/N_o

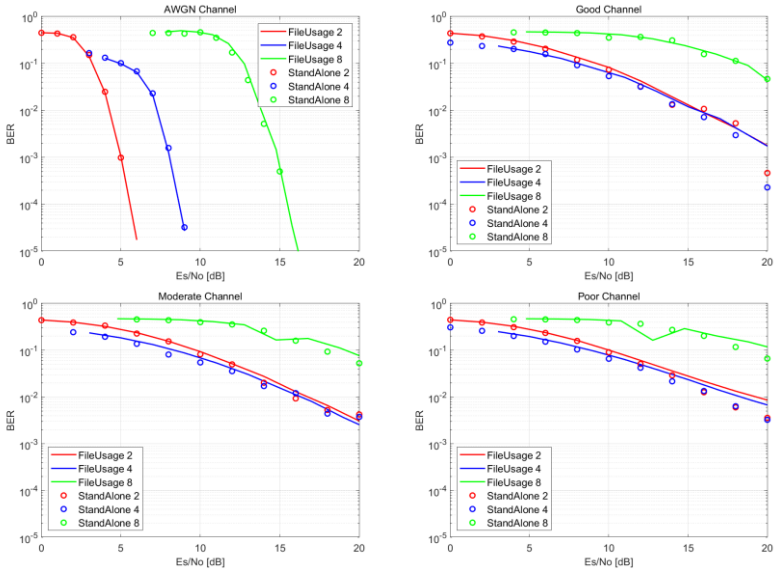


Рис. 3. *BER* в зависимости от E_s/N_o

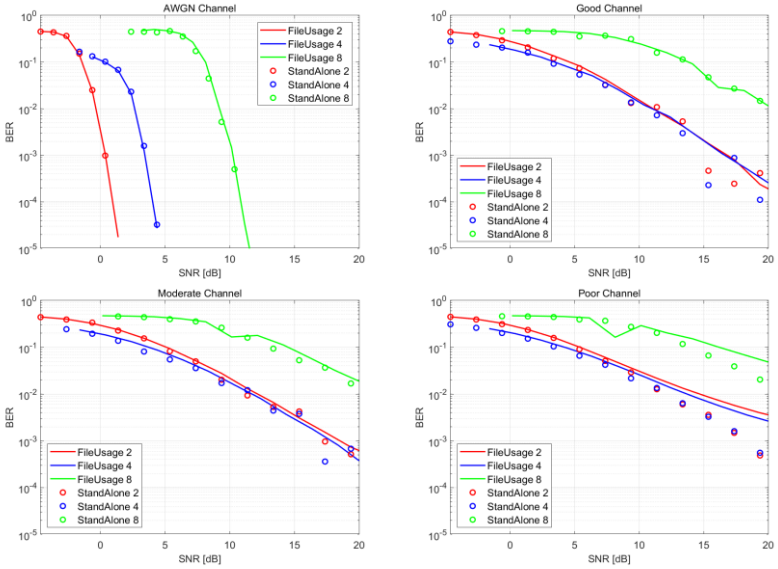


Рис. 4. *BER* в зависимости от *SNR*

Выводы

Результаты эксперимента показывают, что модели канала полностью совпадают в канале с АБГШ и достаточно близко совпадают в каналах с замираниями. Наибольшие расхождения присутствуют в *poor channel* при отношениях сигнал/шум более 15 дБ, что свидетельствует о различной реализации механизма многолучевого распространения сигнала в исследуемых моделях.

Полученные результаты подтверждают, что модель канала из [3] может использоваться для проверки работоспособности АПД в лабораторных условиях. Безусловно эти проверки не могут полностью заменить трассовые испытания, но позволяют существенно уменьшить стоимость и сроки разработки систем цифровой радиосвязи.

Построенные кривые помехоустойчивости описывают сигнальный уровень АПД из [3] и могут быть использованы для разработки методов передачи данных или оценки применимости стриминговых сервисов (широковещательные аудио или видео трансляции). Эти кривые специально представлены для трех часто используемых способов определения отношения сигнал/шум: *SNR*, E_s/N_o и E_b/N_o, что упрощает сравнение с АПД других производителей.

Для выяснения, почему кривые помехоустойчивости начинают расходиться с ростом отношения сигнал/шум, необходимо сравнивать модели каналов без использования АПД, например: исследовать расширение спектра на гармонических сигналах.

Литература

1. F.1487: Testing of HF modems with bandwidths of up to about 12 kHz using ionospheric channel simulators URL: https://www.itu.int/rec/R-REC-F.1487/en (дата обращения 3 сентября 2020).

2. F.520: Use of high frequency ionospheric channel simulators URL: https://www.itu.int/rec/R-REC-F.520/en (дата обращения 3 сентября 2020).

3. Шаптала В.С., Солнцев Д.В. Модель фрагмента сети цифровой радиосвязи // Техника средств связи. 2020. № 2 (150). С. 71-79.

4. Сергиенко А.Б. Цифровая связь: Учебное пособие. СПб.: СПБГЭТУ "ЛЭТИ". 2012. 164 с.

References

1. F.1487: Testing of HF modems with bandwidths of up to about 12 kHz using ionospheric channel simulators URL: https://www.itu.int/rec/R-REC-F.1487/en (accessed 3 Sep. 2020).

2. F.520: Use of high frequency ionospheric channel simulators URL: https://www.itu.int/rec/R-REC-F.520/en (accessed 3 Sep. 2020).

3. Shaptala V.S., Solntsev D.V. Model of pilot area of digital radio network. Means of communication equipment. 2020. NO 2 (150). P. 71-79 (in Russian).

4. Sergienko A.B. Digital Communication: A Tutorial SPB: Saint-Petersburg Electrotechnical University "LETI", 2012. 164 c. (in Russian).

Статья поступила 03 сентября 2020 г.

Информация об авторах

Шаптала Василий Сергеевич – Кандидат технических наук. Начальник лаборатории ПАО «Интелтех». E–mail: shaptalavs@inteltech.ru.

Соколов Владимир Александрович – Ведущий инженер ПАО «Интелтех». E–mail: sokolovva@inteltech.ru.

Машкин Андрей Игоревич – Магистр СПбГЭТУ «ЛЭТИ». Инженер ПАО «Интелтех». E–mail: mashkinAI@inteltech.ru. Адрес: 197342, г. Санкт-Петербург, Кантемировская ул., д. 8. Тел. 8 (812) 448-19-01.

Using of the signal-code construction of data transmission equipment for comparing models of radio channel

V.S. Shaptala, V.A. Sokolov, A.I. Mashkin

Annotation. *The article aims to compare the bit error rate of a multichannel packet modem obtained in two ways: using the built-in functions of the MATLAB technical calculation system and using the channel model from the pilot area of the digital radio communication network. The main goal of this work is to obtain the bit error rates for the main types of the radio channel in accordance with the recommendation ITU-R F 1487. The methods of cross-platform programming and digital signal processing are used in the simulation. The novelty of the discussed solution is in the comparison of two radio channel models made in accordance with the ITU-R F 1487 recommendation. The results of the paper include the bit error rate graphs of the modem being developed. The practical significance of the work consists in the possibility of demonstrating the modem without real radio channels and the possibility of comparing modems of different performers in laboratory.*

Keywords: *bit error rate; signal-code construction; digital signal processing; shortwave frequency band.*

Information about Authors

Shaptala Vasily Sergeevich – Ph.D. in communications. Head of laboratory PJSC “Inteltech”. E–mail: shaptalavs@inteltech.ru.

Sokolov Vladimir Alexandrovich – Lead engineer of PJSC “Inteltech”. E–mail: sokolovva@inteltech.ru.

Mashkin Andrey Igorevich – Master of Saint-Petersburg Electrotechnical University "LETI". Software engineer of PJSC “Inteltech”. E–mail: mashkinAI@inteltech.ru. Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya street 8, Tel. 8 (812) 448-19-01.

Для цитирования: Шаптала В.С., Машкин А.И., Соколов В.А. Использование сигнально-кодовой конструкции аппаратуры передачи данных для сравнения моделей радиоканала // Техника средств связи. 2020. № 3 (151). С. 37-42.

For citation: Shaptala V.S., Mashkin A.I., Sokolov V.A. Using of the signal-code construction of data transmission equipment for comparing models of radio channel. Means of communication equipment. 2020. No 3 (151). Pp. 37-42 (in Russian).

УДК 621.396.93

Формирование спектрально-эффективного сигнала

Солозобов С.А., Шевченко В.В., Щукин А.Н.

Аннотация. *В работе рассматривается новый подход к формированию спектрально эффективных сигналов, основанный на дополнительном преобразовании сформированного сигнала со скачкообразным изменением его фазы, с использованием непрерывного вейвлет-преобразования. Приведена математическая модель сигнала на выходе квадратурного модулятора и выражения для определения его энергетического спектра. Представлено разложение сформированного сигнала на выходе квадратурного модулятора в базисе функций, сформированных из материнского вейвлета. Проведено имитационное моделирование источника формирования информационной последовательности, процесса формирования и анализа сигнала на выходе квадратурного модулятора. Осуществлена сравнительная оценка сформированных сигналов по ширине, занимаемого ими спектра. Результаты работы могут быть реализованы при создании перспективных радиопередающих устройств декаметрового диапазона волн.*

Ключевые слова: *декаметровые волны; математическая модель; квадратурный модулятор; вейвлет-преобразование; ширина спектра.*

Введение

Развитие систем декаметровой связи невозможно без использования в средствах радиосвязи, составляющих их основу, спектрально-эффективных сигналов. Особенно остро эта проблема стоит перед разработчиками систем радиосвязи, располагающих сильно ограниченным частотным ресурсом. К таким системам, в силу различных обстоятельств, относятся системы декаметровой радиосвязи. Так, узкая полоса частот, пригодных для связи в декаметровом диапазоне волн в ночное и дневное время, приводит к её высокой загруженности, вследствие чего создаётся сложная помеховая обстановка для работающих в ней радиолиний. Следовательно, необходимо повышать эффективность использования частотного спектра, выделенного для системы радиосвязи.

Одним из способов роста эффективности при использовании спектра частот является сужение ширины спектра частот полезного сигнала [1], необходимого для обеспечения приема информации с требуемой достоверностью.

Радиолинии декаметровой связи, использующие сигналы с широким спектром частот, в большей степени подвержены воздействию на них случайных и преднамеренных помех, которые негативно влияют на качество приема информации.

Одним из показателей эффективности сигнала, используемого в системах радиосвязи, является спектральная эффективность, которая характеризуется полосой частот, необходимой для передачи информации с определенной скоростью [1].

Существуют различные методы повышения спектральной эффективности сигналов, используемых в различных системах радиосвязи [1], [2]. Одним из них является метод получения спектрально-эффективных сигналов, т. е. сигналов, энергия которых сконцентрирована в узкой полосе частот при заданной скорости передачи. Это достигается путем сглаживания фронтов импульсных последовательностей, поступающих на вход модулятора.

Разработка сигналов, обладающих достаточно высокой спектральной эффективностью, является не только актуальной задачей, но практически полезной для специалистов в области радиосвязи вообще, и, декаметровой радиосвязи в частности.

1 Математическая модель сигнала с квадратурной модуляцией

В условиях возрастающих требований к цифровым системам связи возникает необходимость в максимально возможном ограничении спектра частот сигнала передатчика и повышению его спектральной эффективности.

Ограничение спектра сигнала на выходе модулятора происходит при помощи формирующего фильтра. Ограничение спектра сигнала влияет на точность восстановления его формы в точке приема.

Для восстановления, приемлемой для принятия решения формы импульса в точке приема необходимо, чтобы в ограниченном формирующим фильтром спектре сигнала было сосредоточено не менее 97 % его энергии.

Рассмотрим сигнал, формируемый в квадратурном модуляторе.

Математическая модель сигнала *QPSK* (*quadrature phase shift keying*) с амплитудой A_0, средней несущей частотой ω при условии независимого формирования квадратурных составляющих может быть записана следующим образом

$$Y(t) = A_0\, a(t)(d_i \cos(\omega t+\varphi_0)+d_q \sin(\omega t+\varphi_0)), \quad (1)$$

где A_0 – амплитуда огибающей $a(t)$; $\omega = 2\pi f$ – частота на которой формируется сигнал; d_i и d_q – значения бит сообщения, принимающих значения «1» и «–1» с длительностью T;
φ_0 - начальная фаза гармонического колебания.

Сигнал $Y(t)$ является случайным, так как символы сообщения, поступающие на вход квадратурного модулятора, изменяются по случайному закону.

Спектр реализации случайного процесса (1) определяется выражением [3]

$$F_y(\omega) = \int_{-T}^{T} Y(t) * \exp(-j\,\omega t)dt, \quad (2)$$

где T – длительность сигнала $Y(t)$.

Спектральная плотность мощности случайного процесса равна [3]

$$S_y(\omega) = \lim_{T\to\infty} \frac{E[|Fy(\omega)|^2]}{2T}, \quad (3)$$

односторонняя спектральная плотность мощности случайного процесса, для положительных частотных составляющих спектра f, имеет вид

$$G_y(f) = 2\, S_y(2\pi f). \quad (4)$$

Ширина спектра сигнала зависит от скорости передачи информации, а именно, от скорости изменения модулируемого параметра. Следовательно, для сужения спектра необходимо, чтобы параметр частоты, на которой формируется сигнал, изменялся медленно.

Одним из современных методов анализа спектров радиосигналов является метод вейвлет-анализа.

Проведем анализ *QPSK* сигнала с использованием вейвлет-преобразования.

Преобразуем сформированный сигнал в одномерном непрерывном базисе функций, сконструированных из материнского вейвлета.

Непрерывное вейвлет-преобразование (НВП) определяется выражением [4]

$$C(\tau, s) = \frac{1}{\sqrt{s}} \int_{-\infty}^{\infty} Y(t)\, \Psi\left(\frac{t-\tau}{s}\right) dt = \frac{1}{\sqrt{s}} \int_{n\Delta t}^{n\Delta t+sN\Delta t} Y(t)\, \Psi\left(\frac{t-\tau}{s}\right) dt, \quad (5)$$

где: $\Psi\left(\frac{t-\tau}{s}\right)$ – вейвлет-функция, сконструированная из материнского вейвлета; τ – параметр сдвига вейвлет-функции по оси времени; s – масштаб вейвлет-функции, то есть ее ширина по оси времени; Δt – интервал дискретизации сигнала; n – номера отсчетов входного сигнала; N – уровень разложения по масштабу.

Следует отметить, что при фиксированном масштабе, т. е. когда $s = s_0$, $C(\tau, s_0)$ будет характеризовать временную зависимость преобразованного сигнала с коэффициентами, определяемыми выражением

$$C(\tau, s_0) = \frac{1}{\sqrt{s_0}} \int_{n\Delta t}^{n\Delta t + s_0 N\Delta t} Y(t)\, \Psi\left(\frac{t-\tau}{s_0}\right) dt. \quad (6)$$

Таким образом, зафиксировав масштаб базисной функции, получим исходный сигнал во временной области со сглаженными скачками фазы сформированного *QPSK* сигнала.

В качестве материнского вейлвета, целесообразно использовать вейвлет наиболее точно совпадающего с формой преобразуемого сигнала.

Процесс НВП заключается в перемещении материнского вейвлета по оси времени, где определен сигнал, с постоянным масштабом и вычисление коэффициентов входного сигнала в соответствии с выражением (6). Перемещение материнского вейвлета осуществляется с интервалом, соответствующим произведению $s_{0*} N * \Delta t$. В точках, где нет скачка фазы сигнал на выходе вейвлет-преобразователя точно соответствует сигналу на его входе. В точках, где есть скачек фазы сигнала, вейвлет-преобразователь сглаживает изменение фазы в соответствии с законом изменения базисной функции.

Таким образом, зафиксировав масштаб (величина обратная частоте, на которой сформирован сигнал) и перемещая вейвлет-функцию вдоль оси времени со сдвигом, равным интервалу $s_{0*} N * \Delta t$, получим преобразованный исходный входной сигнал во временной области.

Из-за масштабирования и временного сдвига ($\tau / s_0 = \text{const}$) сохраняется относительная «плотность» расположения базисных вейвлет-функций по оси времени, что обеспечивает качественный анализ преобразуемого входного сигнала.

Особенностью данного подхода является то, что для сохранения $\tau / s_0 = \text{const}$ необходимо, чтобы частота, на которой формируется сигнал, была кратна скорости передачи информации. Для обеспечения постоянного количества отсчетов, при изменении скорости передачи, на длительности символа сформированного *QPSK* сигнала, с целью сохранения энергии на длительности символа, необходимо, чтобы количество периодов на его длительности было постоянным. При этом, должно выполняться равенство

$$N = T*f = f/R, \quad (7)$$

где: R – скорость передачи информации.

Из выражения (7) следует, что при постоянном значении N увеличение скорости передачи информации приводит к увеличению частоты f, на которой формируется сигнал *QPSK*.

2 Моделирование процесса формирования *QPSK* сигнала

Моделирование процесса формирования и анализа сигнала *QPSK* проводилась в среде *Matlab*.

В качестве источника информации используются два датчика случайных последовательностей, формируемых сигналы «-1» и «1» со скоростью символов 500 символ/с.

Математическая модель *QPSK* сигнала, представленная выражением (1), использовалась для формирования исследуемого сигнала.

Базисные функции сформированы из материнского вейвлета Морле, как наиболее точно совпадающие с формой преобразуемого сигнала [4].

Моделирование проводилось для входных сигналов без сглаживания фронтов дискретных сигналов, со сглаживанием и с вейвлет преобразованием сформированного *QPSK* сигнала без сглаживания фронтов.

Результаты моделирования процесса $Y(t)$ при $a(t) = 1$ и вычисление его спектральной плотности мощности в приложении *Matlab* показаны на рис. 1.

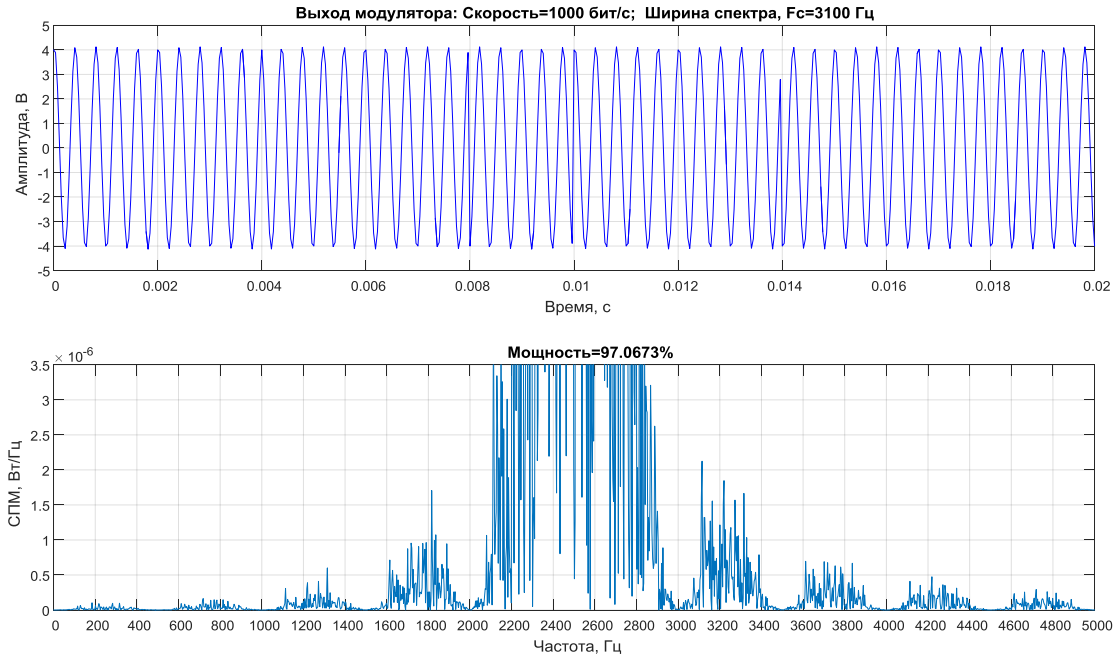


Рис. 1. Временной и спектральный графики $Y(t)$ при $a(t) = 1$

Результаты моделирования процесса $Y(t)$ при изменяющейся на длительности бита T_c амплитуды по закону $a(t) = \sin(\pi t/T)$ и вычисление его спектральной плотности мощности в приложении *MatLab* показаны на рис. 2.

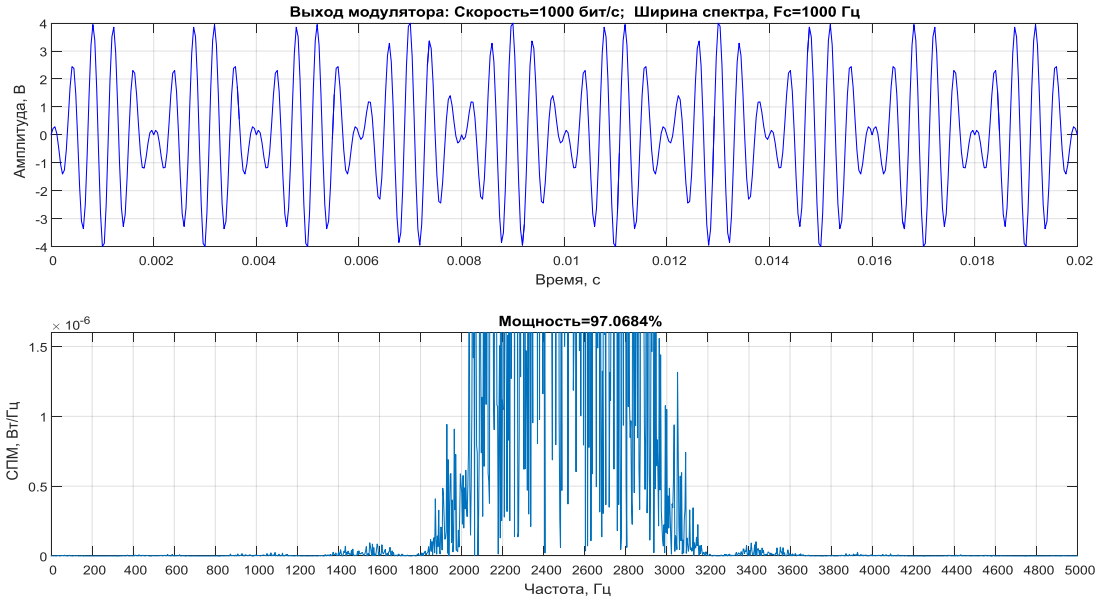


Рис. 2. Временной и спектральный графики $Y(t)$ при $a(t) \neq 1$

Результаты моделирования процесса $Y(t)$ при $a(t) = C(\tau, s_0)$, одномерном вейвлет-преобразовании в базисе материнского вейвлета Морле и вычисление его спектральной плотности мощности в приложении *MatLab* показаны на рис. 3.

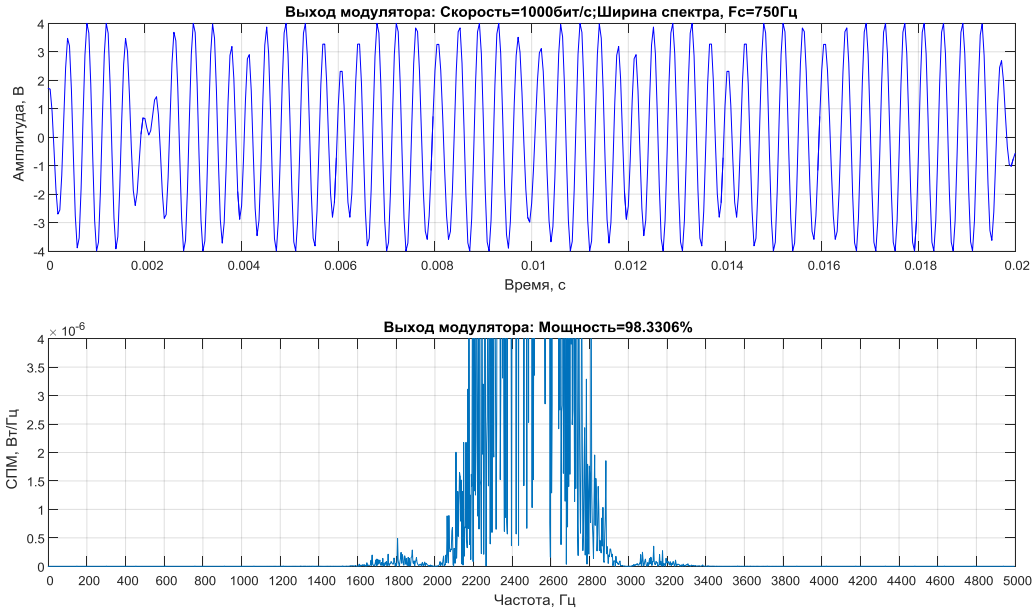


Рис. 3. Временной и спектральный графики $Y(t)$ при использовании материнского вейвлета Морле

Из верхней части рис. 1 и 3 видно, что в результате вейвлет-преобразования сигнала в верхней части рис. 1 происходит плавное сглаживание скачков его фазы (верхняя часть рис. 3). В результате этого ширина спектра преобразованного сигнала уменьшается более чем в четыре раза. Длительность импульса при таком преобразовании не изменяется и равна $1/R$.

Для восстановления формы сигнала, с целью принятия решения на приемной стороне «какой символ передавался» необходимо, чтобы в спектре сформированного сигнала, его мощность составляла не менее 97 %.

По результатам моделирования, была проведена оценка выигрыша по ширине спектра сигналов $QPSK_{НВП}$ с непрерывным вейвлет-преобразованием по сравнению с $QPSK$ без сглаживания фронтов импульсов и $QPSK_{СГ}$ со сглаживанием фронтов импульсов на выходе полосового фильтра, который оценивался как отношение полос занимаемых спектрами исследуемых сигналов без сглаживания входных импульсов, со сглаживанием по закону $a(t) = \sin(\pi t/T)$ и с использованием НВП. Выражение для оценки выигрыша по ширине спектра имеет вид

$$K^{A} = \Delta F_{QPSK\,(СГ)}{}^{A} / \Delta F_{QPSKНВП}{}^{A}, \quad (8)$$

где: A – число показывающее процент, учитываемых частотных составляющих спектра сигнала; $\Delta F_{QPSK\,(СГ)}{}^{A}$ – ширина спектра сигнала без сглаживания входных импульсов и со сглаживанием входных импульсов по закону $a(t) = \sin(\pi t/T)$, соответственно; $\Delta F_{QPSKНВП}{}^{A}$ - ширина спектра сигнала с НВП.

Используя выражение (6) и значения ширины спектра сигналов, показанных на рис. 1, 2, 3, определим их эффективность $К^{97\%}=\Delta F_{QPSK(СГ)}{}^{97\%}/\Delta F_{QPSKНВП}{}^{97\%}$

Результаты расчета приведены в табл. 1.

Таблица 1 – Результаты расчета

Сигналы	$QPSK$	$QPSK_{СГ}$	$QPSK_{НВП}$
$QPSK$	1		
$QPSK_{СГ}$	3,1	1	
$QPSK_{НВП}$	4,13	1,33	1

Из результатов, приведенных в табл. 1 видно, что для $QPSK_{НВП}$ значение 4,13 указывает на то, что для учета 97 % частотных составляющих спектра, ширина спектра частот сигнала *QPSK* должна быть в 4,13 раза, а $QPSK_{СГ}$ со сглаживанием в 1,33 раза шире ширины чем спектр частот сигнала $QPSK_{НВП}$.

Проведена также оценка спектральной эффективности сигналов $QPSK_{НВП}$ по сравнению с *QPSK* и $QPSK_{СГ}$, которая оценивалась как отношение скорости передачи к ширине спектра сигнала, в котором сосредоточено не менее 97 % его мощности. Выражение для оценки спектральной эффективности имеет вид

$$\gamma^{97\%} = R_{QPSK(СГ),\,НВП}^{97\,\%} / \Delta F_{QPSK\,(СГ),\,НВП}^{97\%}$$

Результаты расчета приведены в табл. 2.

Таблица 2 – Результаты расчета

Сигналы	*QPSK*	$QPSK_{СГ}$	$QPSK_{НВП}$
QPSK	0,32		
$QPSK_{СГ}$		1	
$QPSK_{НВП}$			1,33

Из результатов, приведенных в табл. 2 видно, что при квадратурной модуляции спектральная эффективность для $QPSK_{НВП}$ составляет 1,33, для $QPSK_{СГ}$ – 1, для *QPSK* – 0,32. Это указывает на то, что при использовании $QPSK_{НВП}$ сигнала можно передавать 1,33 бита, $QPSK_{СГ}$ – 1 бит, *QPSK* – 0,32 бита в полосе частот 1 Гц.

Выводы

1) Результаты моделирования показывают, что вейвлет-преобразование сигнала на выходе квадратурного модулятора позволяет уменьшить полосу пропускания радиолинии, в которой этот сигнал используется на 25 % по сравнению с радиолинией, использующей сигнал $QPSK_{СГ}$ и на 313 % – *QPSK*. В результате этого, уменьшается уровень шумов на входе демодулятора приемника, что существенно сказывается на качество приема информации, а также приводит к рациональному использованию выделенного частотного ресурса.

2) Для реализации квадратурного модулятора с непрерывным вейвлет-преобразованием необходимо на его выходе установить модуль, обеспечивающий разложение сигнала в базисе материнской вейвлет Морле, как наиболее близко совпадающей с ним по форме.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

2. Макаров С.Б., Завьялов С.В. Оптимизация формы огибающей спектрально-эффективных многочастотных сигналов // Электромагнитные волны и электронные системы. 2014. № 7. Т. 19. – М.: 2014. С. 38 – 45.

3. Купер Дж., Макгиллем К. Вероятностные методы анализа сигналов и систем: Пер. с англ. – М.: Мир. 1989. – 376 с.

4. Смоленцев Н.К. Основы теории вейвлетов. Вейвлеты в MATLAB. – М.: ДМК Пресс. 2009. – 448 с.

References

1. Sklyar B. *Cifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie* [Digital communication. Theoretical foundations and practical application]. ISPR.: Per. s Engl. Moscow. publishing house "Williams", 2003. 1104 p. (in Russian).

2. Makarov S.B. and Zav'yalov S.V. *Optimizaciya formy ogibayushchej spektral'no-effektivnyh mnogochastotnyh signalov* [Optimization of the shape of the envelope of the spectral-efficient multi-

frequency signals]. Electromagnetic waves and electronic systems. Vol. 7. Vol. 19. 2014. Moscow. 2014. Pp. 38 – 45 (in Russian).

3. Cooper J., Mcgillem K. *Veroyatnostnye metody analiza signalov i sistem* [Probabilistic methods of signals and systems]. Per. from English. Moscow. Mir, 1989. 376 p. (in Russian).

4. Smolentsev N.K. *Osnovy teorii vejvletov. Vejvlety v MATLAB* [Fundamentals of wavelet theory. Wavelets in MATLAB]. Moscow. DMK Press, 2009. 448 p. (in Russian).

Статья поступила 07 сентября 2020 г.

Информация об авторах

Солозобов Сергей Анатольевич – Кандидат технических наук, доцент. Начальник научно-исследовательского отдела ПАО «Интелтех». E-mail: solozobob@inteltech.ru. Тел. (812) 295-40-54.

Шевченко Василий Васильевич – Кандидат военных наук, доцент. Начальник лаборатории ПАО «Интелтех». E-mail: ShevchekoVV@inteltech.ru. Тел. (812) 448-95-94.

Щукин Анатолий Николаевич – Кандидат технических наук. Главный специалист ПАО «Интелтех». E–mail: ShchukinAN@inteltech.ru. Тел. (812) 448-95-94.

Адрес: 197342, Россия, г. Санкт Петербург, ул. Кантемировская, д. 8.

Generation of spectral-efficient signal

S.A. Solozobov, V.V. Shevchenko, A.N. Shchukin

Annotation. *The purpose of this work is to show how using the continuous wavelet transform method it is possible to improve the spectral efficiency of a signal with a jump-like change in the phase of the modulated oscillation. A mathematical model of the signal at the output of a quadrature modulator and an expression for determining its energy spectrum is given. The decomposition of the generated signal at the output of a quadrature modulator in the basis of functions formed from the parent wavelet is presented. Simulation modeling of the source of information sequence formation, the process of signal formation and analysis at the output of the quadrature modulator is carried out. A comparative assessment of the generated signals by the width of the spectrum they occupy is carried out. The criterion of spectral efficiency of the simulated signals is chosen as the efficiency criterion. The results of simulation modeling of the formation process and analysis of generated signals are presented. The paper considers a new approach to the formation of spectrally efficient signals based on an additional transformation of the generated signal with a jump-like change in its phase, using a continuous wavelet transform. The results of the work can be implemented when creating promising radio transmitting devices of the decameter wave range.*

Keywords: *decameter waves; mathematical model; quadrature modulator; wavelet transform; spectrum width.*

Information about Authors

Sergey Anatolyevich Solozobov – Doctoral. The postgraduate shef of the Department Inteltech. Tel.: +7 (812) 295-40-54. E–mail: solozobob@inteltech.ru.

Vasiliy Vasilievich Shevchenko – Doctoral. The postgraduate shef of the Department Inteltech. Tel.: +7 (812) 448-95-94. E–mail: ShevchekoVV@inteltech.ru.

Anatoliy Nikolaevich Shchukin – Doctoral. The postgraduate engenier of the Department Inteltech. Tel.: +7 (812) 448-95-94. E–mail: ShchukinAN @inteltech.ru.

Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya st., 8.

Для цитирования: Солозобов С.А., Шевченко В.В., Щукин А.Н. Формирование спектрально-эффективного сигнала // Техника средств связи. 2020. № 3 (151). С. 43-49.

For citation: Solozobov S.A., Shevchenko V.V. Shchukin A.N. Generation of spectral-efficient signal. Means of communication equipment. 2020. No 3 (151). Pp. 43-49 (in Russian).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.53

Основные проблемы обеспечения информационной безопасности в ведомственных информационно-вычислительных сетях в условиях цифровизации предоставления услуг пользователям сетей

Миронов А.А., Салюк Д.В.

Аннотация. *Представлен комплексный подход к обеспечению информационной безопасности в информационно-вычислительных сетях, учитывающий совокупность различных факторов. С помощью модели совокупностей компонентов распределенной среды, соединенных между собой соединительными линиями (каналами передачи данных), определены места воздействия нарушителя на информационные потоки в информационно-вычислительных сетях, определяющие возможные каналы несанкционированного получения информации. Определены каналы утечки информации в ведомственной информационно-вычислительной сети, включающие большое число компонент, в которых циркулируют информационные потоки различной степени конфиденциальности, в условиях активного внедрения цифровых технологий в процедуры предоставления услуг гражданам Российской Федерации. Это вызывает необходимость усиления мер по комплексной защите информации от различных угроз несанкционированного воздействия. Возможные места воздействия нарушителя на информационные потоки в информационно-вычислительных сетях представлены моделью совокупностей компонентов распределенной среды, соединенных между собой соединительными линиями (каналами передачи данных). Дана классификация угроз безопасности и особенности их реализации в функциях уровней модели взаимодействия открытых систем. Приведена совокупность угроз безопасности и их классификация по определенным признакам, уточнены их цели. Выявлены основные особенности и проблемы обеспечения информационной безопасности в системе передачи данных информационно-вычислительных сетей. Выявлены первоочередные проблемы обеспечения безопасности, которые обусловлены особенностями построения и функционирования информационно-вычислительных сетей. Обоснована защита перспективной информационно-вычислительной сети на этапе планирования, как единый комплекс мер, охватывающий процесс обработки информации на всех уровнях. Показано, что разработка политики безопасности, ее реализация и управление защитой должны подчиняться общей концепции защиты. В выводах установлено, что в условиях необходимости цифровизации процессов предоставления услуг потребителям увеличивается актуальность разработки и реализации механизмов комплексного подхода к обеспечению информационной безопасности.*

Ключевые слова: *информационная безопасность; ведомственные информационно-вычислительные сети; каналы утечки информации; угрозы безопасности.*

Введение

Представлен комплексный подход к обеспечению информационной безопасности в информационно-вычислительных сетях, учитывающий совокупность различных факторов. С помощью модели совокупностей компонентов распределенной среды, соединенных между собой соединительными линиями (каналами передачи данных), определены места воздействия нарушителя на информационные потоки в информационно-вычислительных сетях (ИВС), определяющие возможные каналы несанкционированного получения информации.

Дана классификация угроз безопасности и особенности их реализации в функциях уровней модели взаимодействия открытых систем.

1 Каналы утечки информации в ведомственной ИВС

Информационно-вычислительная сеть, включающая в себя большое число компонент, в которых циркулируют информационные потоки различной степени конфиденциальности, в условиях активного внедрения цифровых технологий в процедуры предоставления услуг

гражданам Российской Федерации вызывает необходимость усиления мер по комплексной защите информации от различных угроз несанкционированного воздействия [1].

К числу структурных компонентов ИВС, на которых реализуются различные угрозы, относятся: персональные электронно-вычислительные машины (ПЭВМ), выполняющие функции абонентских терминалов и сетевых устройств, а также технические средства локальных сетей и систем передачи данных, соединительные линии, каналы связи и др. Указанные средства разнесены в пространстве и могут эксплуатироваться в условиях открытого доступа, что создает множество возможных каналов утечки информации, и, тем самым, возможность реализации угроз безопасности ИВС.

Для успешного решения проблем обеспечения информационной безопасности ИВС должностное лицо, ответственное за безопасность, должно иметь ясную картину о всех возможных каналах несанкционированного получения информации, а также угрозах безопасности, которые могут привести к тому, что требования к ИВС, в части информационной безопасности, при отсутствии защиты, окажутся не выполнены. Данное обстоятельство дает возможность злоумышленнику доступ к информации, подлежащей защите, включая персональные данные пользователей услуг.

Возможные места воздействия нарушителя на информационные потоки, в ИВС можно проиллюстрировать моделью совокупностей компонентов распределенной среды, соединенных между собой соединительными линиями (каналами передачи данных), рис. 1. Каналы связи, используемые в системе передачи данных (СПД) ИВС, в наибольшей степени доступны для реализации нарушителем угроз безопасности с целью получения конфиденциальной информации или ее модификации, что может привести к отказу ИВС в предоставлении услуг пользователям. Кроме того, при этом предполагается, что в распределенной среде есть нарушитель, имеющий полномочия пользователя и не имеющий таковых, который имеет набор технических средств и соответствующего программного обеспечения, позволяющих реализовать перехват информации, наблюдать за процессом ее передачи и приема, модифицировать, уничтожать, производить задержку сообщений, производить изменение маршрута и дублировать процесс передачи.

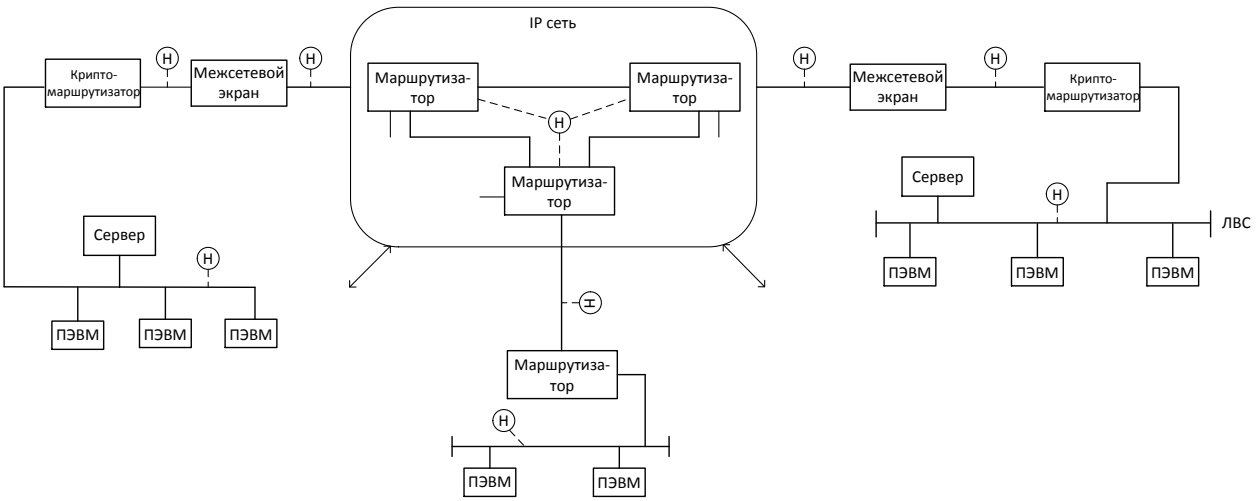


Рис. 1. Возможные места реализации угроз обеспечения информационной безопасности в общей структуре ИВС

Знание всего множества каналов несанкционированного получения информации и возможностей ее модификации определяет выбор механизмов защиты, обеспечивающих уровень защиты, в соответствии с требованиями системы обеспечения безопасности в ведомственной ИВС. Следует отметить, что угроза нарушения безопасности существует в любой точке коммуникации ИВС.

В связи с этим, наиболее важно исключить каналы утечки в технических средствах обработки и коммуникаций ИВС, в которых информация циркулирует в открытом виде. К ним, прежде всего, относятся: оконечное оборудование данных, терминальные устройства, ПЭВМ, устройства коммутации и соединительные линии.

По каналам утечки с перечисленного оборудования нарушитель имеет возможность:

- копировать и похищать носители информации;
- получать информацию с использованием методов, реализующих несанкционированный доступ (НСД) с рабочих мест пользователей;
- получать информацию с использованием средств акустического анализа и визуального наблюдения;
- получать информацию по каналам электромагнитного излучения с технических средств;
- получать информацию с использованием высокочастотного электромагнитного навязывания;
- получать информацию по каналам переходных наводок на оборудование, не относящееся к ИВС, но расположенное вблизи от технических устройств ИВС и имеющее выход за пределы зоны, контролируемой службой безопасности (сети электропитания, теплоснабжения, радиофикации и др.).

Наличие таких каналов обусловливается реальными возможностями технических средств перехвата и обработки информации, поэтому защита информации должна быть обеспечена разработкой и реализацией организационных и инженерно-технических мероприятий, которые должны регламентироваться с учетом требований к уровню защиты.

К другой группе каналов утечки относятся каналы, причиной которых являются ошибки соответствующих должностных лиц (администратора безопасности, программиста, оператора) в процессе эксплуатации и обслуживании технических средств ИВС.

Такими каналами являются:

- утечка информации, вследствие неисправности аппаратуры;
- утечка информации в результате сбоев в программах обработки и передачи;
- утечка информации в результате ошибочной коммутации;
- утечка информации в результате нарушения режима секретности и правил пользования защищаемыми техническими средствами.

Перекрытие указанных каналов утечки должно осуществляться с использованием организационных мероприятий, которые должны быть разработаны и реализованы с учетом ведомственных инструкций по режиму обеспечения конфиденциальности.

Защита содержания информации от утечки путем электромагнитного излучения с линий связи, физического подключения к линии связи, переходных наводок должна быть обеспечена с использованием криптографических преобразований информации, реализуемых программными, аппаратными или аппаратно-программными средствами.

2 Краткая характеристика угроз безопасности

Под угрозой безопасности будем понимать меру возможности воздействия на ИВС, следствием которого может быть потеря одного или всех признаков, характеризующих свойства безопасности ИВС. Реализацию угроз принято называть атакой.

Определение совокупности возможных угроз и атак необходимо для разработки адекватных мер защиты информации в перспективных ИВС различных ведомств, учитывающих существенное увеличение цифровизации услуг пользователям [2].

Совокупность угроз безопасности можно классифицировать по следующим признакам:

1) по цели реализации угроз;
2) по принципу воздействия на ИВС;

3) по характеру атаки на ИВС;
4) по способу воздействия на объект атаки;
5) по объекту атаки;
6) по типу используемого программного обеспечения;
7) по содержанию задачи реализации угроз.

В зависимости от модели нарушителя, возможны и другие классификационные признаки угроз.

Реализация той или иной угрозы может преследовать следующие цели:

1) нарушение конфиденциальности;
2) нарушение целостности;
3) нарушение работоспособности ИВС, в целом.

Нарушение конфиденциальности может привести к разглашению конфиденциальных данных ведомства и персональных данных пользователей.

Классификация угроз безопасности ИВС приведена на рис. 2.

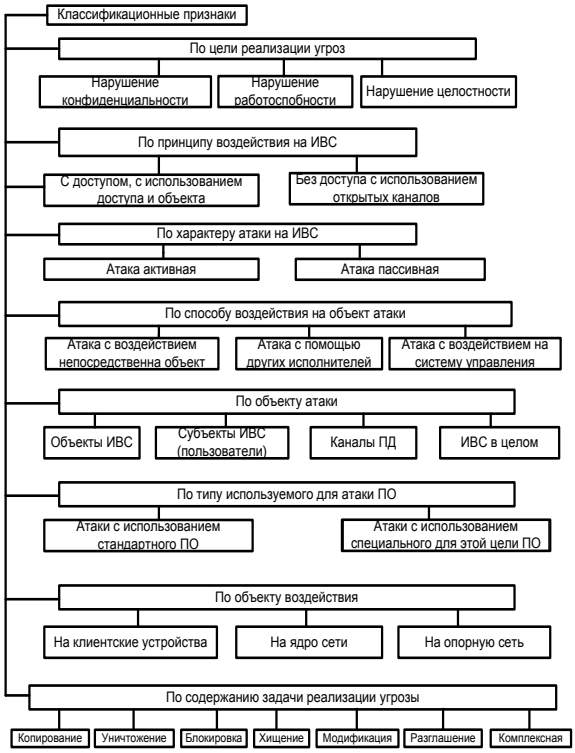


Рис. 2. Классификация угроз безопасности ИВС

Нарушение целостности может привести к тому, что важная информация может быть обесценена или утрачена путем ее несанкционированного удаления или модификации.

Нарушение работоспособности приводит к отказу в обслуживании и предоставлении услуг пользователям ИВС.

Реализация принципа воздействия на ИВС возможна с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, запоминающим устройствам, каналам связи, техническим средствам коммутации и др.) и без использования доступа, с использованием скрытых каналов.

При реализации угрозы с использованием доступа формируется информационный поток между субъектом и объектом доступа, приводящий к изменению реализации некоторых функциональных задач ИВС.

Атака без использования доступа субъекта ИВС к объекту осуществляет чтение или запись информации другого процесса с помощью промежуточных объектов. Такая атака

отличается трудностями в организации, меньшей информативностью для нарушителя, сложностью обнаружения и устранения для администратора безопасности.

По характеру воздействия на ИВС различают атаки активные и пассивные. При активной атаке нарушитель выполняет какие-либо действия, выходящие за рамки его обязанностей и нарушающих существующую в ИВС политику безопасности. При этом возможна подмена информации, ее модификация, изменения порядка следования сообщений и т. д.

Пассивная угроза реализуется путем наблюдения различных процессов в ИВС и их анализа. Такая атака не приводит к нарушению решения функциональных задач, а чаще всего приводит к нарушению конфиденциальности данных, циркулирующих в ИВС.

По способу воздействия на объект атаки различают: атаки с непосредственным воздействием, атаки с воздействием через других пользователей, атаки с воздействием через систему разрешений.

Непосредственное воздействие на объект атаки, например, непосредственный доступ к набору данных, программе, службе, каналу связи и др., обычно легко предотвратить с помощью средств контроля доступа. Атака с помощью других исполнителей осуществляется двумя путями: в первом случае, пользователь присваивает каким-либо образом полномочия другого пользователя, выдавая себя за него (маскарад); во втором случае, один пользователь заставляет другого выполнить необходимые действия (которые для системы защиты не выглядят несанкционированными), причем последний о них и не подозревает. Для реализации этой угрозы может использоваться вирус (вирус выполняет необходимые действия, и передает информацию тому, кто ее внедрил).

Указанные оба способа атаки чрезвычайно опасны, поэтому при разработке системы безопасности перспективной ИВС должны быть предусмотрены меры по их предотвращению. В частности, требуется постоянный контроль пользователей со стороны администраторов сети за набором и передачей данных.

Объектами атаки могут быть: ИВС в целом, объекты ИВС, субъекты ИВС, каналы передачи данных.

При атаке на ИВС, в целом, злоумышленник пытается проникнуть в систему для реализации несанкционированных действий, приводящих к нарушению ее работоспособности.

Объекты ИВС – данные или программы в оперативной памяти или на внешних носителях. Воздействия на объекты системы обычно имеют целью нарушение конфиденциальности и целостности обрабатываемой и хранимой информации.

Субъекты ИВС – процессы пользователей. Целью атак на субъекты ИВС является приостановка работы, изменение привилегий пользователей или характеристик процессов пользователей.

Атаки на каналы передачи данных могут привести к нарушению трафика работы сети, вводу ложной информации, дезорганизующей работу пользователей и сети, в целом, нарушению порядка доступа и конфиденциальности информации. Для защиты от таких атак должны быть реализованы системно–технические решения с использованием механизмов криптографической защиты.

По типу используемого программного обеспечения различаются атаки с использованием стандартного программного обеспечения и с использованием программ, специально разработанных для атаки. Атаки с использованием специальных программ затруднены, поскольку хорошо изучены, и для защиты от них разработаны эффективные методы защиты. Атаки с использованием специально разработанных программ особенно опасны, поэтому все новое программное обеспечение по обработке конфиденциальной информации в ИВС должно внедряться только после проведения соответствующих работ специализированной организацией.

Приведенный перечень угроз безопасности свидетельствует о необходимости комплексного подхода к разработке и реализации мер по обеспечению информационной безопасности в ИВС, поскольку не существует универсального способа, который предотвратил бы всю совокупность возможных атак, последствия которых могут привести к их успешной реализации.

3 Основные особенности и проблемы обеспечения информационной безопасности в системе передачи данных информационно-вычислительной сети

Наличие угроз и каналов утечки вызывает необходимость включения функций обеспечения информационной безопасности в число обязательных требований к ИВС. Данное обстоятельство порождает необходимость решения следующих проблем обеспечения безопасности, обусловленных особенностями построения и функционирования ИВС:

- совместное использование многими пользователями территориально разнесенных ресурсов ИВС увеличивает риски НСД и требует применения большего числа элементов и механизмов защиты;
- объединение различных подсистем ИВС в единую сеть, а также комбинация различных программно-аппаратных средств, увеличивает уязвимость в отношении безопасности системы в целом, и, тем самым, повышает риски в обеспечении защиты информации;
- возможность изменения структуры сети, путем подключения новых телекоммуникационных узлов и технических средств пользователей услуг, увеличивает границы сети и, тем самым, увеличивает вероятность реализации угроз безопасности;
- возможность получения доступа к ИВС в коммуникационных узлах и центрах коммутации пакетов, а также получения доступа в коммутируемых линиях связи и модемов, увеличивает количество возможных точек атак, и затрудняет идентификацию нарушителя;

В связи с этим, защита в перспективной ИВС должна планироваться как единый комплекс мер, охватывающий процесс обработки информации на всех уровнях, а разработка политики безопасности, ее реализация и управление защитой должны подчиняться общей концепции защиты.

Для каждого типа коммуникационного узла сети СПД ИВС должны быть разработаны совокупность услуг безопасности и механизмов их реализации, с учетом выполняемых функций и требований сети.

На каждом коммуникационном узле необходимо обеспечить:

1) контроль доступа к файлам и данным, доступным из локальных сетей и других функциональных узлов;
2) контроль процессов, инициализированных с удаленных узлов;
3) контроль сетевого трафика;
4) идентификация и аутентификация трафика;
5) контроль доступа к ресурсам узла техническим персоналом и пользователями сети;
6) контроль за распределением информации в пределах локальной сети и связанных с нею других сетей.

Поскольку ИВС будет развиваться как совокупность, в том числе, и обособленных систем, сопрягающихся между собой с использованием протоколов всех уровней модели открытых систем, то средства защиты целесообразно рассматривать как применительно к уровням этой модели, так и комплексно к ИВС [3].

Функции защиты информации каждого уровня должны быть реализованы, с учетом особенностей работы процедур протоколов каждого уровня и общих требований к защите информации в ИВС.

Процессы физического и канального уровня, обеспечивающие функциональные, электрические, и процедурные задачи установления, поддержания и разъединения соединения служат звеном между каналом связи, вносящим ошибки, и протоколами более высоких уровней, обеспечивающих безошибочную передачу данных. Указанные процессы реализуются двумя компонентами: аппаратной сетевой картой и соответствующим драйвером сетевого интерфейса. Вместе они обеспечивают как физическое подключение к кабелю (или другой физической среде), так и управление всеми аппаратными процессами передачи. В качестве вероятных угроз, на этом уровне возможны: несанкционированное подключение, ошибочная коммутация, модификация информации, внесение неисправности в канал связи, переадресование и др.

Защита от указанных процессов осуществляется, в основном, шифрованием сообщений, шифрованием соединения, трафика или его выборочной части.

Сетевой уровень отвечает за перемещение пакетов по тому или иному маршруту ИВС. В семействе протоколов *TCP/IP* сетевой уровень представлен в основном, протоколами *IP, ICMP, IGMP*. К угрозам на сетевом уровне следует отнести: возможный анализ незарегистрированным пользователем топологии и служебной информации сети, модификация таблиц маршрутизации и *IP* – адресов.

Для обеспечения информационной безопасности на сетевом уровне необходима идентификация услуг сервиса безопасности (аутентификация, контроль доступа, конфиденциальность потока, целостность и сохранность данных) с использованием механизмов криптографии.

Транспортный уровень организует для вышестоящего прикладного уровня обмен данными между двумя ПЭВМ ИВС. Для чего, в семействе протоколов *TCP/IP* используются два существенно различных транспортных протокола: *TCP* – протокол управления передачей и *UDP* – протокол дейтаграмм пользователя. *TCP* обеспечивает надежную передачу потоков данных между двумя ПЭВМ. *TCP* решает все проблемы надежной доставки врученных ему данных по назначению. *UDP* рассылает данные адресатам в виде пакетов (*UDP*-дейтаграмм) без гарантий их доставки. Для обеспечения безопасности на транспортном уровне необходимо обеспечить контроль доступа к приложениям (в составе межсетевого экрана), механизмы аутентификации данных с применением механизмов криптографии.

Протоколами прикладного уровня обеспечивается выполнение различных сервисов (задач). В их числе: *Telnet*-протокол удаленного доступа; *FTP* – протокол передачи файлов, *SMTP* – простой протокол обмена электронной почтой; *SNMP* – простой протокол управления сетью и др. В общем случае, на прикладном уровне реализуются процедуры передачи, маршрутизации разборки/сборки пакетов, а также механизмы обеспечения целостности и аутентификации пользователей и процессов. К основным угрозам на прикладном уровне следует отнести: НСД к данным, модификацию правил разграничения доступа, имитацию. В связи с этим, механизмами обеспечения информационной безопасности на прикладном уровне являются механизмы, использующие криптографию.

Заключение

В условиях необходимости цифровизации процессов предоставления услуг, потребителям увеличивается актуальность разработки и реализации механизмов комплексного подхода к обеспечению информационной безопасности.

Поскольку не существует универсального способа, который предотвратил бы всю совокупность возможных атак, последствия которых могут привести к их успешной реализации, при разработке системы обеспечения информационной безопасности с требуемой степенью конфиденциальности, целесообразно ранжировать уровни угроз и «стоимость» для потребителя их реализации в ИВС.

Литература

1. Таненбаум Э., Уэзеролл А. Компьютерные сети. – СПб.: Питер, 2017.
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000.
3. Стивенс У.Р. Протоколы TCP/IP. Пер. с англ. и коммент. А.Ю. Глебовского. – СПб.: «Невский Диалект» - «БХВ-Петербург», 2003.

References

1. Tanenbaum Je., Ujezeroll A. *Komp'yuternye seti* [Komp'juternye seti]. St. Petersburg. Piter. 2017 (in Russian).
2. Petrov A.A. *Komp'yuternaya bezopasnost'. Kriptograficheskie metody zashchity* [Komp'juternaja bezopasnost'. Kriptograficheskie metody zashhity]. Moscow. DMK. 2000 (in Russian).
3. Stivens U.R. Protokoly TCP/IP. Per. s angl. i komment. A.Ju. Glebovskogo. St. Petersburg «Nevskij Dialekt» – «BHV-Peterburg». 2003 (in Russian).

Статья поступила 11 сентября 2020 г.

Информация об авторах

Миронов Анатолий Анатольевич – Кандидат технических наук, доцент. Инженер первой категории ПАО «Интелтех». Тел.: +79111131524. E–mail: saldv@inteltech.ru.

Салюк Дмитрий Владиславович – Кандидат технических наук, доцент. Начальник отдела ПАО «Интелтех». Тел.: +79217941064. E–mail: saldv@inteltech.ru.

Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

The main problems of ensuring information security in departmental information and computing networks in the conditions of "digitalization" providing services to network users

A.A. Mironov, D.V. Salyuk

Annotation. *A comprehensive approach to ensuring information security in information and computing networks is presented, taking into account a set of various factors. Using the model of components of distributed medium connected to each other by connecting lines (data transmission channels), the places of influence of the intruder on information flows in the information processing system are determined, which determine possible channels of unauthorized information acquisition. Information leakage channels have been identified in departmental IVS, which include a large number of components in which information flows of various degrees of confidentiality circulate, in the conditions of the active introduction of digital technologies in the procedures for providing services to citizens of the Russian Federation. This makes it necessary to strengthen measures for the integrated protection of information against various threats of unauthorized influence. Possible locations of the intruder's influence on information flows in the IVS are represented by a model of sets of distributed medium components connected to each other by connecting lines (data channels). The classification of security threats and their specific implementation in functions of layers of the model of interaction of open systems are given. A set of security threats and their classification according to certain signs are given, their goals are specified. The main features and problems of ensuring information security in the DPA of the IVS were identified. Priority security problems have been identified, which are due to the peculiarities of the construction and operation of the IVS. The protection of prospective IVS at the planning stage is justified, as a single set of measures covering the process of processing information at all levels. It is shown that the development of a security policy, its implementation and protection management should be subject to the general concept of protection. The conclusions found that in the context of the need to digitalize "the processes of providing services to consumers, the relevance of developing and implementing mechanisms for an integrated approach to ensuring information security is increasing.*

Keywords*: information security; departmental information-computing networks; information leakage channels; security threats.*

Information about Authors

Mironov Anatoly Anatolyevich – Candidate of technical sciences, associate professor. Engineer of the category of PJSC Inteltekh. Tel.: + 79111131524. E-mail: saldv@inteltech.ru.

Salyuk Dmitry Vladislavovich – Candidate of technical sciences, associate professor. Head of equestrian and business PJSC «Inteltekh». Tel.: + 79217941064. E-mail: saldv@inteltech.ru.

Address: 197342, Russia, St. Petersburg, Kantemirovskaya St., 8.

Для цитирования: Миронов А.А., Салюк Д.В. Основные проблемы обеспечения информационной безопасности в ведомственных информационно-вычислительных сетях в условиях «цифровизации» предоставления услуг пользователям сетей // Техника средств связи. 2020. № 3 (151). С. 50-57.

For citation: Mironov A.A., Salyuk D.V. The main problems of ensuring information security in departmental information and computing networks in the conditions of "digitalization" providing services to network users. Means of communication equipment. 2020. No 3 (151). Pp. 50-57 (in Russian).

УДК 621.391

Идентификация состояния узлов информационно-телекоммуникационных сетей общего пользования подсистемой мониторинга информационной безопасности

Аллакин В.В., Будко Н.П.

Аннотация: Постановка задачи: *на основе многоуровневого подхода к описанию сложных технических систем обосновать моделирование опасных и критических событий информационной безопасности элементов и узлов информационно-телекоммуникационных сетей общего пользования.* ***Цель работы:*** *повышение эффективности функционирования подсистемы мониторинга информационной безопасности информационно-телекоммуникационной системы на различных логических уровнях её структуры.* ***Используемые методы:*** *методы анализа, методы общей теории систем, методы теории игр, методы теории надежности, методы теории нечётких множеств, методы теории вероятностей и математической статистики, методы теории классификации, методы теории графов.* ***Новизна*** *исследования состоит в том, предложена многоуровневая модель наступления критического события информационной безопасности как на информационно-телекоммуникационной системе, так и на отдельных её элементах. Представлен вероятностный граф возникновения несанкционированного доступа к элементам информационно-телекоммуникационной сети случайного либо целенаправленного нарушителя. Обоснованы и описаны аналитически четыре класса состояния информационной безопасности системы с учётом ошибок контроля первого и второго рода. Получено математическое выражение для оценки вероятностей вскрытия и нормального функционирования информационно-телекоммуникационной сети.* ***Результат*** *проведенного исследования состоит в том, что предложенный метод оценки информационной безопасности позволяет получить численную оценку защищенности информационно-телекоммуникационной сети в условиях неполной информации о нарушителе и его возможностях, при этом использован подход, позволяющий учесть и рассмотреть воздействия угроз информационной безопасности на разных уровнях системы, не привязываясь к точке входа в неё.*

Ключевые слова: *информационно-телекоммуникационная сеть; подсистема мониторинга; логический уровень сети;ошибки первого и второго рода; информационная безопасность.*

Введение

Современные информационно-телекоммуникационные системы (ИТКС) и сети общего пользования, в которых постоянно наращиваются возможности проведения кибервоздействий, как со стороны организованных международных террористических группировок, так и со стороны вероятного противника (нарушителя) [1-4], представляют концепцию организации и построения элементов (узлов), взаимодействующих друг с другом и внешней средой. Применение технологий измерения, передачи, обработки и идентификации данных обуславливает потребность в создания различных подсистем контроля и мониторинга состояния элементов сети с точки зрения информационной безопасности (ИБ), направленных на нейтрализацию опасного либо критического состояния по причине воздействия внешних, а также внутренних дестабилизирующих факторов или угроз.

Цель статьи: моделирование опасных и критических событий информационной безопасности информационно-телекоммуникационной системы. При этом под *опасным* событием на каждом логическом уровне ИТКС понимается воздействие угрозы ИБ на её элемент, не повлекшее компрометацию его входных и выходных величин, а под *критическим* событием – воздействие, повлекшее компрометацию его входных и выходных величин, что влечёт повышение вероятности вскрытия соседних элементов информационного тракта ИТКС.

Многоуровневый подход к построению структуры ИТКС

Эффективность обеспечения нормального состояния (функционирования) ИТКС во многом зависит от реализации комплексного похода к построению сетевой инфраструктуры на основе соответствующего моделирования угроз ИБ, выбору адекватных средств защиты узлов

(элементов) и каналов связи, методов мониторинга и управления на сети и др. [5-9]. Поскольку известно, что современные ИТКС работают на глобальном, региональном и локальном уровнях, для моделирования её информационного тракта (ИТ) используем многоуровневый подход к построению защиты территориально-распределенной системы. Так на рис. 1 приведена логическая схема функционирования ИТКС в виде информационного тракта доступа из локальной вычислительной сети (локальный уровень – ЛВС) к глобальной компьютерной сети (глобальный уровень – ГКС «Интернет»). На представленной схеме показано, что доступ к тому или иному узлу ИТКС осуществляется по ИТ, через соседние её узлы, имеющие связность с ним и расположенные на сопрягаемых логических уровнях («локальный-региональный», «региональный-глобальный»). При этом на рисунке показаны: I – логический уровень, на котором обеспечивается доступ пользователей в ИТКС (к её ресурсам) при решении прикладных задач; II – логический уровень, занимающий промежуточное звено между ЛВС и ГКС, решающий задачи коммутации и маршрутизации; III – логический уровень сопряжения с ГКС.

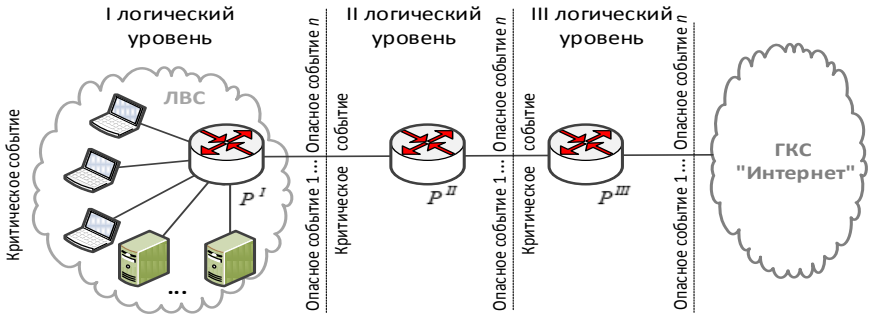


Рис. 1. Логическая схема функционирования информационного тракта ИТКС

Из анализа данной схемы видно, что любая атака, проводимая на первом логическом уровне ИТКС, является критическим событием, поскольку фактически нарушитель работает внутри ЛВС (является внутренним нарушителем) системы. Атаки на объекты II и III логических уровней ИТ ИТКС ожидаемы, ввиду территориальной распределённости системы, это дает возможность осуществления более тщательной подготовки организационных и технических мероприятий по обеспечению их информационной безопасности. В зависимости от целей реализации угроз информационной безопасности, а также их места проведения, имеется возможность выбора и реализации мер защиты и оценки степени их опасности или критичности.

Как рассмотрено во многих работах [1-9] программно-аппаратные средства элементов ИТКС в глобальном киберпространстве постоянно подвержены деструктивным воздействиям, носящим преднамеренный или случайный характер. При этом на различные элементы и узлы ИТКС, типа ПЭВМ, сервер, маршрутизатор, коммутатор, и др., действуют соответствующие виды угроз информационной безопасности [10]. Важно отметить, что одинаковые виды угроз на разных элементах ИТКС и её логических уровнях имеют разную степень критичности их реализаций по нанесению ущерба, как самой ИТКС, так и её системе управления. Соответственно, одна и та же угроза ИБ, действующая на разных логических уровнях ИТКС будет иметь различный уровень опасности (критичности). Поэтому и методы защиты логического уровня либо всей системы вцелом от разных угроз ИБ должны отличаться. Для выбора адекватных мер защиты ИТКС от угроз ИБ на различных её логических уровнях необходимо осуществить моделирование наступления критического события ИБ, а также оценку вероятности его отсутствия (нормального функционирования системы). Далее рассмотрим вопросы моделирования критических событий ИБ на ИТКС и её логических уровнях.

Многоуровневое моделирование критического состояния ИТКС

В предметной области обеспечения ИБ предлагается большое число решений по построению, как моделей атак, моделей нарушителя, так и моделей объектов защиты [1-8]. Причём критические события ИБ обычно представляется совокупностью нескольких опасных

или причинных событий [11], которые происходят на доступных нарушителю различных логических уровнях ИТКС (рис. 1). Для осуществления оценки вероятности реализации таких событий проводится их иерархическая декомпозиция по уровням информационного тракта ИТКС.

На рис. 1 в виде P^I, P^{II} и P^{III} обозначены вероятности наступления критического события, соответственно на I, II и III логических уровнях информационного тракта ИТКС, которые равны:

$$P^I = 1-(1-P^{II})(1-P_{1.1})(1-P_{1.2})...(1-P_{1.n});$$

$$P^{II} = 1-(1-P^{III})(1-P_{1.1})(1-P_{1.2})...(1-P_{1.n});$$

$$P^{III} = 1-(1-P_{1.1})(1-P_{1.2})...(1-P_{1.n}),$$

где $P_{1.1}$, $P_{1.2}$,…, $P_{1.n}$ – вероятности воздействия деструктивных угроз на элементы ИТКС, а n – количество их видов, которые возможны к применению в информационном тракте ИТКС.

Тогда используя математический аппарат общей теории надежности [12] для перехода нарушителя (н) с одного на другой логический уровень ИТКС с учётом противодействия подсистемы мониторинга (м) ИБ ИТКС на каждом из логических уровней (I, II, III), должны соблюдаться необходимые условия, которые характеризуют эту вероятность. Так, вероятность перехода нарушителя с *III* логического уровня ИТКС на *II* логический уровень будет иметь вид $P_1^{III} = \left(1-\left(1-P_{1.1}\right)\left(1-P_{1.2}\right)...\left(1-P_{1.n}\right)\right)P_{\text{н}}^{III}\,\overline{P_{\text{м}}^{III}}$, а вероятность перехода нарушителя от первого к последующему элементу логического уровня (II): $P_1^{II} = \left(1-\left(1-P_1^{III}\right)\left(1-P_{1.1}\right)\left(1-P_{1.2}\right)...\left(1-P_{1.n}\right)\right)P_{\text{н}}^{II}\,\overline{P_{\text{м}}^{II}}$, [11]. При этом, финальную вероятность вскрытия информационного тракта ИТКС выразим как:

$$P_{\text{вскр.}} = P_1^I = \left(1-\left(1-P_1^{II}\right)\left(1-P_{1.1}\right)\left(1-P_{1.2}\right)...\left(1-P_{1.n}\right)\right)P_{\text{ц}}^I\,\overline{P_{\text{м}}^I}.$$

При переходе по иерархии к более низкому логическому уровню информационного тракта ИТКС критическое состояние (событие) текущего уровня может рассматриваться или опасным событием последующего логического уровня, или критическим событием всей ИТКС. Также, любое из опасных событий с некоторой вероятностью может привести к критическому событию на данном логическом уровне ИТ ИТКС, однако может и не исключать появления последующих *n*-х опасных событий для рассматриваемого сетевого элемента. Это говорит о том, что опасные события для элемента логического уровня ИТ ИТКС являются совместными.

Трансформация критического события ИБ одного логического уровня в опасное событие другого уровня, или же наступление критического события для всего ИТ ИТКС во многом зависит от места возникновения несанкционированного доступа (НСД) нарушителя в нём, технической оснащенности обеих из сторон противоборства, а также применяемых технологий воздействия на ИТКС и доступных методов защиты элементов информационного тракта. При этом важно учитывать и цели информационного воздействия при осуществлении НСД, а так же эффективность функционирования подсистемы мониторинга ИБ ИТКС при обнаружении НСД.

С учетом вышеизложенного, решение задачи оценки эффективности подсистемы мониторинга ИБ ИТКС, предложено представить байесовской игрой с неполной информацией о нарушителе и его предполагаемых стратегиях [13]. При этом модель поведения нарушителя с учетом идентификации НСД подсистемой мониторинга ИБ ИТКС приведена на рис. 2. Из чего видно, что при возникновении НСД к элементу любого логического уровня ИТКС существует вероятность того, что доступ совершён *случайным* или *целенаправленным* нарушителем.

Поскольку известно [1-4], что в ГКС «Интернет» взлом информационных ресурсов стал повседневной проблемой и де-факто проверкой на «профессионализм» нерадивых начинающих пользователей, то в модели будем считать «случайным» нарушителем ($З_{\text{с}}$) нарушителя ИБ, получивший доступ к элементу информационного тракта ИТКС случайным образом (или с целью решения своих задач на вычислительных мощностях «потенциальной жертвы»), а «целенаправленным» нарушителем ($З_{\text{ц}}$) нарушителя-профессионала (хакера), владеющего информацией о целях и задачах информационно-телекоммуникационной системы и её ресурсов.

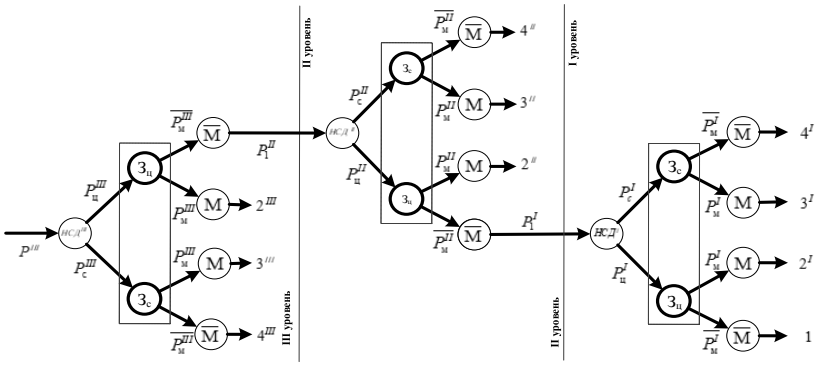


Рис. 2. Модель распознавания критического состояния ИТКС подсистемой мониторинга

Используя подход концепции теории игр [13], первым шаг делает нарушитель. В тоже время, нам неизвестно «случайный» (с) или «целенаправленный» (ц) нарушитель осуществил НСД. Следовательно, в информационное множество рассматриваемой модели мы должны включить оба эти типа нарушителей через вероятности осуществления НСД: $P_{\text{с}}$ и $P_{\text{ц}}$. Также на каждом из элементов ИТ ИТКС существует два состояния системы мониторинга, сводящиеся к финальным вероятностям состояниям элемента на рассматриваемом логическом уровне: $P_{\text{м}}$ – когда система мониторинга обнаруживает НСД; $\overline{P_{\text{м}}}$ – когда система мониторинга не смогла обнаружить НСД. Соответственно, в модели на рис. 2 выделены классы 1 – 4 состояния элемента (узла) информационного тракта ИТКС рассматриваемого логического уровня:

1 – элемент ИТ ИТКС взломан целенаправленным нарушителем, при этом подсистема мониторинга не сообщила о НСД ($\overline{\text{М}}$), противник переходит на следующий логический уровень;

2 – элемент взломан целенаправленным нарушителем, подсистема мониторинга сообщила о факте нарушения ИБ (М), своевременно проводятся меры противодействия НСД;

3 – элемент взломан случайным нарушителем, подсистема мониторинга сообщила о факте нарушения ИБ ИТ ИТКС (М), своевременно проводятся меры противодействия НСД;

4 – элемент взломан случайным нарушителем, подсистема мониторинга не сообщила о факте нарушения ИБ ($\overline{\text{М}}$), нарушитель не переходит на следующий логический уровень ИТКС.

При этом классы состояния ИТКС «2» – «4» являются внутриуровневыми, а класс состояния «1» позволяет целенаправленному нарушителю перейти на следующий уровень ИТКС. В связи с чем, вариационный ряд предпочтения финальных состояний, применимый для рассматриваемого сетевого элемента или для ИТКС в целом имеет вид: $3 \succ 2 \succ 4 \succ 1$, т. е. критическим (наименее предпочтительным) классом состояния ИБ ИТКС будет класс «1».

Аналитически финальные вероятности для элемента логического уровня ИТКС можно записать в виде: $P^*_{\text{"1"}} = P^* P^*_{\text{ц}} \overline{P^*_{\text{м}}}$; $P^*_{\text{"2"}} = P^* P^*_{\text{ц}} P^*_{\text{м}}$; $P^*_{\text{"3"}} = P^* P^*_{\text{с}} P^*_{\text{м}}$; $P^*_{\text{"4"}} = P^* P^*_{\text{с}} \overline{P^*_{\text{м}}}$, где $P_{\text{м}}$ – вероятность идентификации НСД подсистемой мониторинга ИБ ИТКС, * – номер логического уровня ИТКС.

Моделирование событий информационной безопасности на логических уровнях ИТКС

Вероятности проведения деструктивного воздействия на элементы информационного тракта ИТКС – $P_{1.1}$, $P_{1.2}$,…, $P_{1.n}$ зависят от многих факторов как внутреннего состояния элемента ИТКС, свойств подсистемы ИБ, эффективности подсистемы мониторинга, так и возможностей потенциального нарушителя ИБ (видов угроз ИБ элементов ИТКС и используемых методов защиты от них). При этом подсистема мониторинга фактически реализует поэтапную процедуру контроля ИБ на каждом из логических уровней ИТКС, когда на первом этапе происходит *обнаружение* НСД (опасного события), а на втором – *распознавание* критического события.

На рис. 3 обозначены классы критического состояния элементов ИТ ИТКС, где: O – обнаружение опасного события ИБ ИТКС, $O = 1 - \overline{O}$; P_1 – априорная вероятность факта нормального функционирования ИТКС ($\overline{O}$), $P_1 = 1 - P_2$; P_2 – априорная вероятность факта вскрытия ИТКС (O); $\overline{K}$ – нормальное состояние ИБ ИТКС; K – критическое состояние ИБ ИТКС;

α – ошибка первого рода «ложная тревога о НСД» (α = 1 – $\bar{\alpha}$); β – ошибка второго рода «необнаруженный НСД» (β = 1 – $\bar{\beta}$); «1» – ИТКС функционирует нормально, ложное обнаружение НСД не распознано; «2» – ИТКС вскрыта, опасное событие обнаружено, но не распознано; «3» – ИТКС функционирует нормально, ложное обнаружение НСД и распознавание; «4» – ИТКС вскрыта, опасное событие обнаружено и распознан; «5» – ИТКС функционирует нормально, признана работоспособной; «6» – ИТКС вскрыта, но НСД не обнаружено. На рис. 3 также приведены вероятности обнаружения и распознавания критического состояния ИБ ИТ ИТКС.

Надёжностная схема замещения вероятностного графа (по рис. 3) информационного тракта ИТКС с учетом логического уровня подсистемы мониторинга, в функционировании которой также могут наблюдаться ошибки первого α и второго рода β, приведена на рис. 4.

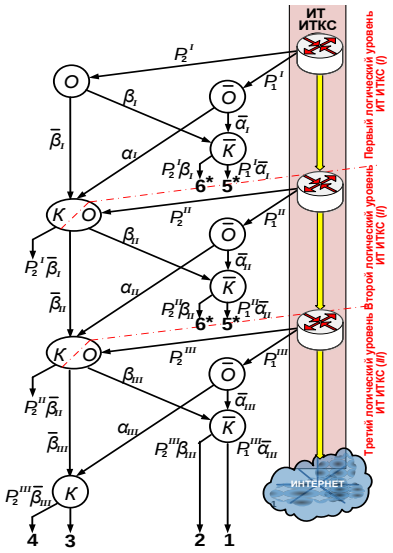


Рис. 3. Вероятностный граф определения класса критического состояния ИТКС

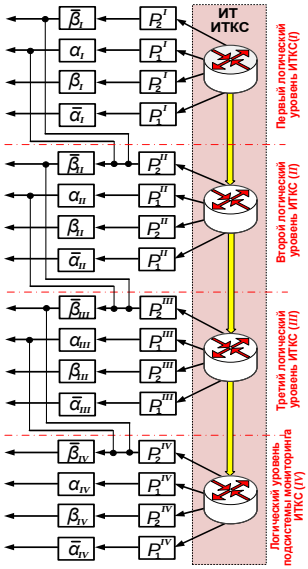


Рис. 4. Надёжностная схема замещения вероятностного графа определения класса критического состояния ИТКС

Процедура определения финальной вероятности нормального функционирования (отсутствия критического состояния ИБ) $P_{нф}$ ИТ ИТКС с учетом ошибок первого и второго рода представлена на рис. 5, а процедура определения финальной вероятности наступления критического события ИБ $P_{кс}$ информационного тракта ИТКС, соответственно, на рис. 6.

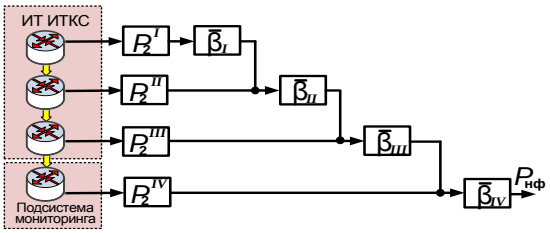


Рис. 5. Процедура определения финальной вероятности отсутствия критического состояния ИБ (нормальное функционирование – $P_{нф}$) ИТКС

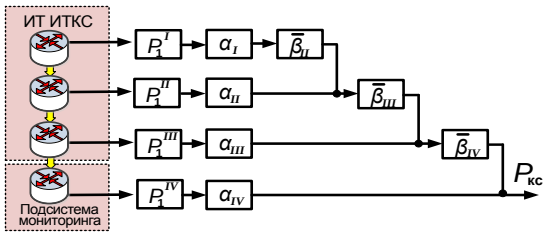


Рис. 6. Процедура определения финальной вероятности наступления критического состояния ($P_{кс}$) ИБ ИТКС

Тогда математические записи расчета $P_{нф}$ и $P_{кс}$ с учетом ошибок контроля ИБ имеют вид:

$$P_{нф} = 1-\left(1-\bar{\beta}_{IV}\left\langle 1-\left[\bar{\beta}_{III}\left\{1-\left(1-P_1^{I}\,\alpha_I\,\bar{\beta}_{II}\right)\left(1-P_1^{II}\,\alpha_{II}\right)\right\}\right]\left[1-P_1^{III}\,\alpha_{III}\right]\right\rangle\right)\left(1-P_1^{IV}\,\alpha_{IV}\right). \quad (1)$$

$$P_{кс} = \left(1-\left\langle 1-\bar{\beta}_{III}\left[1-\bar{\beta}_{II}\left\{1-\left(1-P_2^{I}\,\alpha_I\,\bar{\beta}_I\right)\left(1-P_2^{II}\right)\right\}\right]\left[1-P_2^{III}\right]\right\rangle\left\langle 1-P_2^{IV}\right\rangle\right)\bar{\beta}_{IV}\,. \quad (2)$$

Вывод

В представленном методе идентификации состояния элементов (узлов) ИТКС общего пользования подсистемой мониторинга ИБ можно выделить следующие достоинства:

использован подход «сверху вниз», позволяющий учесть и рассмотреть воздействия угроз информационной безопасности на разных уровнях ИТКС, не привязываясь к точке входа в неё;

осуществлена оценка защищенности ИТКС с учётом ошибок мониторинга ИБ первого и второго рода, когда отсутствует полная информация о нарушителе, а также его возможностях;

модель ИТКС представлена в виде вероятностного графа с строго структурированным и при этом гибким подходом, позволяющим анализировать результаты воздействия случайного или целенаправленного нарушителя информационной безопасности и различных других факторов.

Литература

1. Дементьев В.Е. Угрозы инфотелекоммуникационной сети в условиях информационного противоборства. СПб.: ВАС, 2015.192 с.

2. Коцыняк М.А., Кулешов И.А., Лаута О.С. Устойчивость информационно-телекоммуникационных сетей. СПб.: Изд-во Политехн. ун-та, 2013. 92 с.

3. Анненков В.И., Баранов С.Н., Моисеев В.Ф., Сергеев Н.А. Безопасность и противоборство в информационной сфере. Аспекты национальной безопасности. М.: РУСАВИА. 2010. 446 с.

4. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. СПб.: Наукоемкие технологии, 2017. 546 с.

5. Климов С.М. Методы и модели противодействия компьютерным атакам. Люберцы: Каталист, 2008. 316 с.

6. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью // Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 74-103.

7. Котенко И.В., Саенко И.Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. СПб.: Наука, 2002. №3 (22). С. 84-100.

8. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121-126.

9. Bursztein E., Mitchell J. C. Using strategy objectives for network security analysis. Information Security and Cruptology. Lecture Notes in Computer Science. 2010. V.6151. Springer Berlin Heidelberg. Pp.337-349.

10. Еремеев М.А., Аллакин В.В., Будко Н.П. Модель наступления критического события информационно-коммуникационной системе // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 6. С. 52-60.

11. Бобов М.Н., Горячко Д.Г., Обухович А.А. Оценка рисков информационной безопасности // Информационно-измерительные и управляющие системы. 2016. №4. Т. 14. С. 69-73.

12. Горелик А.В., Ермакова О.П. Основы теории надежности в примерах и задачах. – М.: МИИТ, 2009. 98 с.

13. Колобашкина Л.Б. Основы теории игр. М.: Бином. 2017. 200 с.

References

1. Dementiev V.E. *Ugrozy infotelekommunikacionnoy seti v usloviyah informacionnogo protivoborstva* [Threats of the infotelecommunication network in the conditions of information confrontation]. Saint Peterburg, Military Academy of Communications Publ., 2015. 192 p. (in Russian).

2. Kotseniak M.A., Kuleshov I.A., Lauta O.S. *Ustoychivost informacionno-telekommunikacionnyh setey* [The Stability of information and telecommunication networks]. Saint Peterbur, Politehnicheskii universitet Publ. 2013. 92 p. (in Russian).

3. Annenkov V.I., Baranov S. N., Moiseev V.F., Sergeev N.A. *Bezopasnost i protivoborstvo v informacionnoy sfere. Aspekty nacionalnoy bezopasnosti* [Security and confrontation in the information sphere. Aspects of national security]. Moscow, RUSAVIA Publ., 2010. 446 p. (in Russian).

4. Makarenko S.I. *Informacionnoe protivoborstvo i radioelektronnaya borba v setecentricheskih voynah nachala XXI veka. Monografia* [Information warfare and radio-electronic warfare in network-centric wars of the beginning of the XXI century]. Saint Petersburg. Naukoemkie Tekhnologii Publ., 2017. 546 p. (in Russian).

5. Klimov S.M. *Metody i modeli protivodeystviya kompyuternym atakam* [Methods and models of countering computer attacks]. Lyubertci, Katalis Publ., 2008. 316 p. (in Russian).

6. Kotenko I.V. Intellektualnye mekhanizmy upravleniya kiberbezopasnostyu [Intellectual mechanisms of cybersecurity management]. *Trudy Instituta sistemnogo analiza Rossijskoi akademii nauk*. 2009. Vol. 41. Pp. 74-103 (in Russian).

7. Kotenko I.V., Sajenko I.B. Postrojenie sistemy intellektualnyh servisov dlia zaschity informatsii v usloviah kiberneticheskogo protivoborstva [Building a system of intelligent services for information protection in the conditions of cybernetic confrontation]. *Trugy SPIIRAN*, 2002, no. 3 (22), pp. 84-100 (in Russian).

8. Sajenko I.B., Biriukov M.A., Efimov V.V., Yasinski S.A. Model administrirovaniya skhem razgranicheniya dostupa v oblachnyh infrastrukturah [Administration Model schemes of access control in cloud infrastructures]. *Informatsiya i kosmos*, 2017, No. 1, pp.121-126 (in Russian).

9. Bursztein E., Mitchell J.C. Using strategy objectives for network security analysis. Information Security and Cruptology. Lecture Notes in Computer Science. 2010. V.6151. Springer Berlin Heidelberg. Pp.337-349.

10. Eremeev M.A., Allakin V.V., Budko N.P. Model nastupleniya kriticheskogo sobytiya informacionno-kommunikacionnoy sisteme [Model of the onset of a critical event in the information and communication system]. *H&ES Research*, 2017, vol. 9, no. 6, pp. 52-60 (in Russian).

11. Bobov M.N., Goriachko D.G., Obuhovich A.A. Otsenka riskov informatsionnoi bezopasnosti avtomatizirovannyh sistem [Assessment of information security risks]. *Informatsionno-izmeritelnye i upravliauschie sistemy*, 2016, vol. 14, no. 4, pp. 69-73 (in Russian).

12. Gorelik A.V., Ermakova O.P. *Osnovy teorii nadiozhnosti v primerah i zadachah* [Fundamentals of reliability theory in examples and problems]. Moscow, MIIT Publ., 2009. 98 p. (in Russian).

13. Kolobashina L. B. *Osnovy teorii igr* [Fundamentals of the theory of games]. Moscow, Binom Publ., 2017. 200 p. (in Russian).

Статья поступила 14 сентября 2020 года

Информация об авторах

Аллакин Владимир Васильевич – Соискатель ученой степени кандидата технических наук. Независимый специалист. E-mail: vladimir@duduh.ru. Адрес: 188660, Ленинградская обл., Всеволожский район, пос. Бугры, ул. Школьная, дом 11, корп. 1, кв. 510.

Будко Никита Павлович – Соискатель ученой степени кандидата технических наук. Независимый специалист. E-mail: budko62@mail.ru. Адрес: 194064, г. Санкт-Петербург, ул. Бутлерова, 9, корп. 1, кв. 252.

Identification of the state of nodes of public information and telecommunications networks by the information security monitoring subsystem

V.V. Allakin, N.P. Budko

Annotation: Problem statement: *on the basis of a multi-level approach to the description of complex technical systems, to justify the modeling of dangerous and critical events of information security of elements and nodes of public information and telecommunications networks.* ***The purpose of the work*** *is to improve the efficiency of the information security monitoring subsystem of the information and telecommunications system at various logical levels of its structure.* ***Methods used:*** *methods of analysis, methods of general systems theory, methods of game theory, methods of reliability theory, methods of fuzzy set theory, methods of probability theory and mathematical statistics, methods of classification theory, methods of graph theory.* ***The novelty*** *of the research is that a multi-level model of the occurrence of a critical event of information security is proposed both on the information and telecommunications system and on its individual elements. The probabilistic graph of the occurrence of unauthorized access to the elements of the information and telecommunications network of a random or targeted intruder is presented. Four classes of the information security state of the system are justified and described analytically, taking into account control errors of the first and second kind. A mathematical expression is obtained for estimating the probabilities of opening and normal functioning of the information and telecommunications network.* ***The result*** *of the* ***s****tudy is that the method of evaluation of information security allows you to obtain a numerical estimate of the protection of information and telecommunication networks in the conditions of incomplete information about the offender and its capabilities, using an approach that allows to take into account and to consider the effects of information security threats at different levels of the system, without being attached to it.*

Keywords: *information and telecommunications network, monitoring subsystem, logical level of the network, errors of the first and second kind, information security.*

Information about Authors

Allakin Vladimir Vasilyevich – Doctoral Student. Independent Expert. E-mail: vladimir@duduh.ru. Address: 188660, Russia, Leningrad region, Vsevolozhsky district, vil. Buhry, Shkolnaya str., 11, build. 1, sq. 510.

Budko Nikita Pavlovich – Doctoral Student. Independent Expert. E-mail: budko62@mail.ru. Address: 194064, Russia, St. Petersburg, Butlerova str., build. 9/3, sq. 252.

Для цитирования: Аллакин В.В., Будко Н.П. Идентификация состояния узлов информационно-телекоммуникационных сетей общего пользования подсистемой мониторинга информационной безопасности // Техника средств связи. 2020. № 3 (151). С. 58-64.

For citation: Allakin V.V., Budko N.P. Identification of the state of nodes of information and telecommunications networks of general use by the subsystem of information security monitoring. Means of Communication Equipment. 2020. No. 3 (151). Pp. 58-64 (in Russian).

ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ

УДК 004.4'24

Архитектура информационных систем

Сиразетдинов Р.Р., Белоус Д.В.

Аннотация: *В статье рассматриваются различные трактовки понятия «информационная система», описаны признаки разделения информационных систем на одиночные, групповые, корпоративные. Представлена технология распределённого преобразования информации «клиент-сервер» и её недостатки. В качестве дальнейшего развития рассматривается многоуровневая архитектура, которая на сегодняшний день является базовой для продуктов компании «1С», внедряемых в ПАО «Интелтех».*

Ключевые слова: *информационная система; технология «клиент-сервер»; многоуровневая архитектура.*

Успешное развитие современного бизнеса немыслимо без комплексной автоматизации, основой которой является применение новых информационных технологий. Одним из основных практических применений информационных технологий в профессиональной деятельности современного специалиста стала автоматизация управления с применением современных информационных систем (ИС), таких как «1С:УПП», «1С:Документооборот», «1С:РМ» и др. Успешное внедрение и сопровождение современных ИС зависит от правильного понимания концепций, определяющих модель, структуру, выполняемые функции и взаимосвязь компонентов ИС, то есть архитектуры.

В настоящее время существуют различные трактовки понятия «ИС». Преобладают следующие подходы к ее определению:

ИС рассматривается как часть (первая очередь) автоматизированной системы управления (АСУ);

АСУ является частным видом ИС;

ИС фактически отождествляется с АСУ, но использование нового термина подчеркивает применение современных технологий, архитектур и средств, и преследует цель обойти негативную реакцию заказчиков (потребителей) на термин «АСУ», обусловленную во многом отрицательным опытом внедрения всевозможных АСУ на протяжении нескольких десятилетий;

под ИС понимается одна из двух разновидностей целевых систем автоматизации (другую составляют системы реального времени);

ИС называют систему, реализующую информационную технологию.

Ряд авторов также использует термины «автоматизированная информационная система», «информационно-техническая система», «информационно-управляющая система» с целью подчеркнуть использование средств вычислительной техники и типы решаемых задач управления, однако любое управление есть выработка информационных, управляющих и организационных решений, и с этих позиций любая ИС используется в целях управления.

В настоящей статье под ИС понимается совокупность технических, программных, информационных, лингвистических и других средств (по видам обеспечения автоматизированных систем), являющихся результатом работ по автоматизации решения прикладных задач обеспечения управленческой деятельности.

Основными признаками (характерными свойствами) рассматриваемых в настоящей работе ИС являются:

принадлежность к автоматизированным системам;

преобладание интерактивного режима функционирования;

наличие собственной информационной базы;

в большинстве случаев – типовая архитектура в виде совокупности базы данных (БД), системы управления базой данных и ряда функциональных приложений (прикладных программ).

С позиций конструктивно-технологических аспектов ИС предполагают разделение на одиночные, групповые и корпоративные.

Одиночные ИС реализуются как автономные на автоматизированных рабочих местах (АРМ). Такие ИС могут содержать несколько простых приложений, связанных общим информационным фондом. Они рассчитаны на работу одного пользователя или группы пользователей, разделяющих по времени одно рабочее место.

Групповые ИС ориентированы на коллективное использование информации членами одной организационной структуры и, как правило, строятся в рамках локальной вычислительной сети. Локальные сети (ЛС) располагаются на ограниченной территории (управление, здание). К ЛС подключается большинство узлов обработки информации, таких как АРМы, серверы, общие сетевые устройства (например, принтеры). Общий информационный фонд, при этом, представляет собой БД или совокупность файловых документов.

Корпоративные ИС являются развитием групповых систем и ориентированы на территориально разнесенные узлы или региональные сети. Они могут иметь иерархическую структуру, включающую одиночные и групповые ИС. Региональная сеть объединяет ЛС с различной средой передачи, однако, отдельные узлы обработки информации могут подключаться к ней и напрямую. Информационный фонд системы этого уровня поддерживает доступ из групповых и одиночных систем и может быть с ними согласован с заданной степенью актуальности.

Так как групповые и корпоративные ИС функционируют на территориально разнесенных узлах, они могут быть классифицированы как распределенные, а совокупность операций, реализуемых в ИС, является распределенным преобразованием информации.

Под реализацией распределенного преобразования информации применительно к вычислительным сетям понимают:

распределенную базу данных;

распределенную обработку данных.

Распределенная БД есть набор БД, связанных между собой логически, но физически расположенных на нескольких машинах, входящих в одну компьютерную сеть.

Распределенная обработка данных означает отделение прикладных программ (приложений) от выполнения операций над данными. Связь между прикладной программой и процессами выполнения операций над данными реализуется программным обеспечением.

В настоящее время широко распространена распределенная обработка данных на основе технологии «клиент-сервер» – двухуровневая архитектура.

При использовании технологии «клиент-сервер» данные обрабатываются на двух логических уровнях: сервера базы данных и клиентского приложения.

Сервер решает задачи организации и разграничения доступа к данным, резервного копирования и восстановления данных. Сервер должен располагаться на отдельном высокопроизводительном компьютере, который подключен к сети.

Клиентские приложения посылают серверу запросы на получение наборов данных, проводят их обработку (добавление и редактирование данных) и отсылают результат обработки обратно на сервер. Клиентские приложения располагаются на персональных компьютерах, объединенных с сервером средствами удаленного доступа (сетью).

Логика обработки данных в таких ИС находится в виде программ-клиентов, обращающихся к распределенной БД с помощью языка запросов и в виде хранимых процедур в БД.

Такой подход имеет ряд очевидных недостатков: при любом изменении алгоритмов необходимо обновлять клиентское приложение на АРМах пользователей; высокие требования к пропускной способности коммуникационных каналов с сервером; слабая защита данных от взлома, в особенности от недобросовестных пользователей системы; высокая сложность администрирования и настройки рабочих мест пользователей системы; необходимость использовать мощные ПК на клиентских местах; высокая сложность разработки системы из-за необходимости выполнять логику обработки данных и обеспечивать пользовательский интерфейс в одной программе.

Дальнейшим развитием архитектуры «клиент-сервер» является многоуровневая архитектура. Многоуровневые приложения представляют собой распределенные системы удаленного доступа к данным, которые состоят из трех или более уровней (рис. 1).

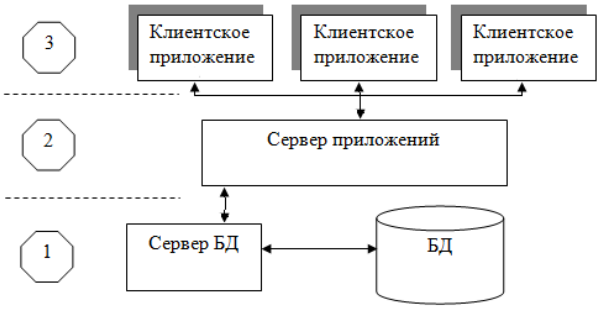


Рис. 1. Структура многоуровневой ИС

Во-первых, это сервер БД, который обеспечивает функционирование используемой приложением БД и непосредственную обработку запросов пользователя.

Во-вторых, это сервер приложений, который составляет так называемое программное обеспечение промежуточного слоя. В общем случае сервер приложений может иметь распределенную структуру и располагаться на нескольких компьютерах.

В-третьих, это совокупность клиентских программ или клиентский уровень приложения. Эти программы выполняют минимальные функции по отображению данных и передаче запросов серверу, а результатов – обратно.

Каждый уровень многоуровневого приложения обеспечивает реализацию одного типа программной логики. Сервер БД содержит логику обработки БД. Сервер приложений берет на себя логику управления потоками данных, организации связи с программами клиентского уровня и применения правил, составляющих уникальную логику обработки данных. Уровень клиентских приложений обеспечивает только взаимодействие с конечным пользователем.

Трехзвенная модель переносит прикладную логику приложения на отдельный уровень сервера приложений. В результате клиентская часть приложения становится «тоньше» и в основном отвечает только за предоставление удобного пользовательского интерфейса, поэтому клиентская часть отличается высокой надежностью и простотой установки.

Как правило, сервер БД также освобождается от необходимости поддерживать функциональность, которая в двухзвенной модели реализуется с помощью специальных расширений системы управления БД, например, хранимых процедур. Это обеспечивает некоторую разгрузку сервера БД за счет применения серверов приложений.

Перенос основных операций приложения на отдельный уровень позволяет с максимальной эффективностью распределить нагрузку на аппаратные средства (приложение на самом деле может быть многозвенным с разделением нагрузки на несколько серверов приложений) и обеспечивает удобное и быстрое наращивание как функциональности приложения, так и числа обслуживаемых пользователей.

Сосредоточение логики обработки данных и системы доступа к данным в сервере приложений позволяет избежать дублирования логики на каждом клиентском приложении.

Для удобства администрирования клиентская программа может быть так же размещена на отдельном сервере, называемом терминальным, при этом на АРМ пользователей настраивается функция удалённого доступа к терминальному серверу.

Иногда в литературе выделяют архитектуру Internet\Intranet, по сути являющуюся разновидностью многоуровневой архитектуры. В этом случае в качестве клиентского приложения используется веб-браузер, взаимодействие которого с сервером приложений обеспечивает веб-сервер.

Литература

1. Ипатов М.Е., Белоус Д.В., Сиразетдинов Р.Р. Система электронного оборота распорядительных и информационно-справочных документов предприятия // Техника средств связи. СПб. 2019. № 1 (145). С. 100-106.

2. Ипатов М.Е., Белоус Д.В., Сиразетдинов Р.Р. Вариант корпоративного портала и системы электронного документооборота предприятия. Новые информационные технологии в системах связи и управления: материалы XV (ежегодной) Российской научно-технической конференции. Калуга. 2016. С. 245 – 247.

3. Петров В.Н. Информационные системы. СПб.: Питер, 2014. 688 с.

4. Емельянова Н.З., Партыка Т.Л., Попов И.И. Проектирование информационных систем: учебное пособие. Москва: Форум: НИЦ ИНФРА-М, 2014. 432 с.

References

1. Ipatov M.E., Belous D.V., Sirazetdinov R.R. The system of electronic circulation of administrative and information-reference documents of the enterprise. Communication equipment. St. Petersburg. 2019. № 1 (145). P. 100-106 (in Russian).

2. Ipatov M.E., Belous D.V., Sirazetdinov R.R. A variant of the corporate portal and the enterprise electronic document management system. New information technologies in communication and control systems: materials of the XV (annual) Russian scientific and technical conference. Kaluga. 2016. P. 245- 247 (in Russian).

3. Petrov V.N. Information Systems. SPb .: Peter, 2014 – 688 p. (in Russian).

4. Emelyanova N.Z., Partyka T.L., Popov I.I. Designing information systems: a tutorial. Moscow. Forum Research Center INFRA-M, 2014. 432 p. (in Russian).

Статья поступила 14 сентября 2020 г.

Информация об авторах

Белоус Денис Васильевич – Кандидат технических наук. Начальник научно-исследовательского отделения ПАО «Интелтех». E-mail: belousdv@inteltech.ru. Тел.: +7 (911) 798-99-70.

Сиразетдинов Рамазан Рафаэлевич – Кандидат технических наук, доцент. Начальник отдела ПАО «Интелтех». E-mail: sirazetdinovrr@inteltech.ru. Тел.: +7 (921) 755-58-68.

Адрес: 197342, Россия, г. Санкт-Петербург, ул. Кантемировская, д. 8.

Information systems architecture

R.R. Sirazetdinov, D.V. Belous

Annotation*: The article discusses various interpretations of the concept of "information system", describes the signs of the division of information systems into single, group, corporate. The technology of distributed transformation of client-server information and its disadvantages are described. As a further development, a multilevel architecture is considered, which today is the base for the products of the 1C company, implemented in PJSC Inteltech.*

Keywords: *information system; client-server technology; multilevel architecture.*

Information about Authors

Belous Denis Vasilievich – Candidate of Technical Sciences. Head of the Research Department of the PJSC «Inteltech». E-mail: belousdv@inteltech.ru. Tel.: +7 (911) 798-99-70.

Sirazetdinov Ramazan Rafaelovich – Candidate of Technical Sciences, Associate Professor. Head of the Research Department of the PJSC «Inteltech». E-mail: sirazetdinovrr@inteltech.ru. Tel.: +7 (921) 755-58-68.

Address: 197342, Russia, St. Petersburg, ul. Kantemirovskaya, 8.

Для цитирования: Сиразетдинов Р.Р., Белоус Д.В. Архитектура информационных систем // Техника средств связи. 2020. № 3 (151). С. 65-68.

For citation: Sirazetdinov R.R., Belous D.V. Information systems architecture. Means of communication equ - ipment. 2020. No 3 (151). Pp. 65-68 (in Russian).

ПЕРСПЕКТИВНЫЕ ИССЛЕДОВАНИЯ

УДК 004.5:681.5

Существование и достижимость консенсуса, как проблема обеспечения надёжности в распределённых геокибернетических платформах

Черный С.Г., Биденко С.И., Якушев Д.И.

Аннотация. *Проблема достижения консенсуса сегодня стала одной из краеугольных при построении надежных распределенных (особенно облачных и блокчейн) приложений и киберфизических систем. Локальные сервисы, как и, в целом, парадигма построения монолитных приложений, ощутимо устарели и больше не в состоянии обеспечить параметры надежности, требуемые современными системами. В статье рассматривается проблема достижения консенсуса на примере семейства алгоритмов «Паксос». Приводятся результаты анализа свойств отдельных алгоритмов, анализа сильных и слабых сторон в различных подходах к усовершенствованию классического алгоритма «Паксос». Доказывается надёжность алгоритма достижения консенсуса.*

Ключевые слова: *надежность; киберфизическая система; управление; территориально распределенная телекоммуникационная система.*

Введение

Современные территориально распределенные геокибернетические платформы [1] широко используют распределенные (параллельные) вычисления [2]. Как и любая современная распределенная информационная система, от простого веб-сайта до модуля сложной поисковой системы, должна отвечать довольно жестким требованиям по надежности, оперативности и доступности. Набирающий популярность микросервисный подход к архитектуре информационных систем требует использования абстракций и не подразумевает обеспечения модуля системы знаниями о топологии и конфигурации целевой системы, то есть модуль не обладает сколь-нибудь полной информацией о распределенной системе [3].

Консенсус в распределённой системе, или распределенный консенсус, требует обеспечения двух основных гарантий [3, 4]:

1) все договоренности окончательны, несмотря на потенциально ненадежное окружение (гарантия надежности);

2) в конечном итоге, договоренность будет достигнута (гарантия прогресса).

Алгоритм Паксос впервые был опубликован в научной литературе в 1998 году и с этого момента фактически стал синонимом распределенного консенсуса. Он широко известен и широко распространен, однако, вместе с тем, часто подвергается критике. Данный алгоритм сложен для понимания, громоздок в реализации, не гибок и может показывать плохую производительность в аварийных ситуациях.

Ниже рассматриваются проблемы достижения консенсуса на примере классического алгоритма Паксос и его модификации.

При этом, напомним основные понятия и соответствующие им англоязычные выражения, используемые при описании систем исследуемого типа: акцептор (*acceptor*), предлагающий (*proposer*), номер раунда (*epoch*), согласованное значение (*agreed/decided value*), принятое значение (*learned value*), предложение (*propose*), обещание (*promise*) [5-7].

1 Теоретические аспекты проблемы распределенного консенсуса

Начнем рассмотрение темы распределенного консенсуса с рассмотрения проблемы достижения консенсуса относительно единственного значения между множеством участников. Не смотря на кажущуюся тривиальность задачи, она является важнейшим компонентом распределенных кибернетических систем [8, 9].

Распределенный консенсус относительно единственного значения – это проблема принятия решения относительно значения $v \in V$ между конечным множеством n участников, $U = \{u_1, u_2, ..., u_n\}$.

Определение 1. Алгоритм считается достигающим распределенного консенсуса, если он удовлетворяет трем требованиям надежности:

1) нетривиальность – согласованное значение должно быть предложено одним из участников;

2) надежность – если значение было согласовано, никакие другие значения согласованы быть не могут;

3) надежность принятия – если участник принимает значение, он обязан принять согласованное значение.

А также двум требованиям прогресса:

1) прогресс – при определенном наборе условий живости (осуществимости), если значение было предложено участником, оно будет в конечном итоге согласованным;

2) принятие в конечном итоге – при определенном наборе условий живости, если значение было согласовано, в конечном итоге оно будет принято.

В совокупности эти условия не позволяют многим тривиальным алгоритмам осуществлять достижение распределенного консенсуса. Без «надежности» и «надежности принятия» алгоритм может принять и решить все значения, предложенные всеми участниками.

Если не требуется «нетривиальность», согласованным значением может быть любая константа.

Если «прогресс» и «принятие в конечном итоге» не требуются, алгоритм может никогда не принять решение, отбрасывая все предложения, либо не позволяя участникам принимать значения [8].

Важно отметить, что свойства надежности не полагаются на условия живости (осуществимости – связи между любыми двумя событиями при выполнении программы распределенных вычислений). То есть, алгоритм не должен полагаться на синхронизацию или на абсолютную надежность компонентов.

Любой участник системы играет одну или сразу обе роли:

1) предлагающий – участник, который предлагает определенные значения;

2) акцептор – участник, который принимает и хранит согласованные значения.

В системе U из n участников обозначим множество акцепторов как $A = \{a_1, a_2, ..., a_n\}$, где $A \subseteq U$, $|a| = n_a$ и множество предлагающих как $P = \{p_1, p_2, ..., p_n\}$, где $P \subseteq n_p$.

Алгоритм консенсуса определяет процесс, при помощи которого значение v выбирается акцепторами, из значений полученных от предлагающих. Мы будем называть время, когда акцепторы определили конкретное значение, точкой соглашения. После этого момента v согласовано и в последствии не может быть изменено. Предлагающие узнают какое значение было согласовано и это всегда должно происходить после точки соглашения.

Классический алгоритм Паксос. Классический Паксос – это алгоритм для решения проблемы распределенного консенсуса. В лучшем случае, алгоритм без оптимизаций может достичь консенсуса за два раунда приема-передачи между большинством акцепторов и за

три синхронных записи в надежное хранилище. Однако, в ряде случаев, времени может потребоваться больше. Условие живости для данного случая может быть выражено в следующей форме: $\left[n_a / 2 \right] + 1$ из n акцепторов и один предлагающий должны быть живы и синхронно сообщаться – данные условия необходимы и достаточны.

Подход классического Паксоса к принятию решения состоит из двух фаз.

1) Первую фазу можно рассматривать как фазу чтения, когда предлагающий изучает текущее состояние системы и выбирает номер версии для определения изменений в будущем.

2) Вторая фаза – фаза записи, когда предлагающий пытается сделать так, чтобы значение было принято.

Если после первой фазы, предлагающий уверен, что значение еще не было согласовано, он может предложить значение γ. Если в итоге первой фазы значение уже может быть согласовано, тогда это значение обязано быть предложенным во второй фазе. Для продолжения необходимо чтобы в каждой из двух фаз большинство акцепторов достигли соглашения.

Определение 2. Номер раунда – это любой член множества номеров E, где E – это любое бесконечное частично-упорядоченное множество, в котором всегда определены операторы $<$, $>$, $=$.

Определение 3. Предложение (e, v) – это пара, состоящая из номера раунда и значения консенсуса.

Первая фаза классического Паксоса:

1) Предлагающий выбирает уникальный номер раунда и отправляет предложение акцепторам в форме сообщения $prepare(e)$.

2) Каждый акцептор сохраняет последний номер раунда и последнее принятое предложение. Когда акцептор получает предложение, если e – первый предложенный номер или если e равно или больше, чем последний предложенный номер, тогда e записывается в хранилище и акцептор отправляет сообщение $promise(e, f, v)$, где (f, v) – это последнее принятое предложение, где f – номер раунда и v – соответствующее предложенное значение.

3) Как только предлагающий получает сообщение вида $promise(e, \cdot, \cdot)$ от большинства акцепторов, он переходит ко второй фазе. Сообщение может содержать в себе последнее принятое предложение, которое будет использовано в следующей фазе.

4) В противном случае, предлагающий ждет определенный период времени и пробует послать сообщение снова с большим значением номера раунда.

Вторая фаза классического Паксоса:

1) теперь предлагающий должен выбрать значение v, следуя правилам:

а) если сообщений $promise(e, \cdot, \cdot)$ не было получено в первой фазе, предлагающий выберет значение-кандидат γ.

б) если одно предложение было получено, выбирается его значение.

в) если было получено более чем одно предложение, тогда предлагающий должен выбрать значение, поступившее с наибольшим номером раунда.

Затем, предлагающий отправляет сообщение $propose(e, v)$ акцепторам.

2) каждый акцептор получает сообщение $propose(e, v)$. Если e – первый предложенный номер, или если e – больше или равен последнему номеру, тогда номер раунда и принятое предложение обновляется и акцептор отправляет сообщение $accept(e)$.

3) Как только предлагающий получает сообщение $accept(e)$ от большинства акцепторов, он принимает значение v как согласованное.

4) В противном случае, предлагающий ждет определенный период времени и возвращается к первой фазе с большим числом раунда.

Алгоритм предлагающего в Классическом Паксосе. Выше было дано описание алгоритма классического Паксоса. Рассмотрим более детально каждую роль. На вход предлагающий получает предложение значения-кандидата γ, на выходе мы получим согласованное значение v. В зависимости от состояния акцепторов во время исполнения алгоритма, значение-кандидат может быть как равно так и не равно согласованному значению. Предлагающий отправляет значение-кандидат γ, только если он уверен, что другое значение пока не было выбрано. Как только предлагающий получает согласованное значение, ни один предлагающий не примет другое согласованное значение.

После инициализации переменных, алгоритм начинает с выбора номера раунда e. Мы не будем останавливаться на том, как выбирается множество возможных номеров раунда, однако необходимо отметить, что алгоритм требует, чтобы каждый номер раунда был использован только единожды [8, 9].

Сообщение $prepare(e)$ отправляется всем акцепторам и предлагающий ждет сообщений в ответ. Если ответ не содержит предложение, тогда максимальный номер раунда $e_{\max}$ и соответствующее значение v не обновляются. Если предложение не принято большинством акцепторов до истечения времени, алгоритм начинает выполняться снова. Если не было получено принятых предложений, v принимает значение γ.

Затем, предлагающий отправляет предложение $propose(e,v)$ акцепторам. Если большинство акцепторов примет предложение (e,v), значение v будет принято предлагающим. В противном случае, алгоритм начнет выполняться снова.

Алгоритм акцептора в Классическом Паксосе. Акцепторы в классическом Паксосе отвечают за обработку входящих сообщений $prepare(\ )$ и $promise(\ )$. Все входящие сообщения должны иметь номер раунда равный или больший, чем номер раунда уже обработанных сообщений. Если сообщение, полученное акцептором первое, то e_{pro} принимает полученное значение e.

Если полученное сообщение $prepare(e)$, то акцептор отвечает сообщением $promise(e, e_{acc}, v_{acc})$. Если предложений пока не было принято, e_{acc} и v_{acc} не будут определены.

Если полученное сообщение $propose(e,v)$, то акцептор выставит e_{acc} и v_{acc} для e и v соответственно. В таком случае, мы будем говорить о том, что акцептор принял предложение (e,v).

Определение 4. В классическом Паксосе предложение (e,v) считается согласованным, если предложение (e,v) было принято большинством акцепторов.

Пример исполнения алгоритма Классического Паксоса. На рис. 1 приведена диаграмма последовательности сообщений как пример идеального случая выполнения классического Паксоса. Сначала предлагающий p_1 проходит алгоритм, где договаривается о предложении $(0,A)$. Затем, алгоритм проходит предлагающий p_2 и договаривается о предложении $(1,A)$. Оба предлагающих затем могут завершить обе фазы классического Паксоса.

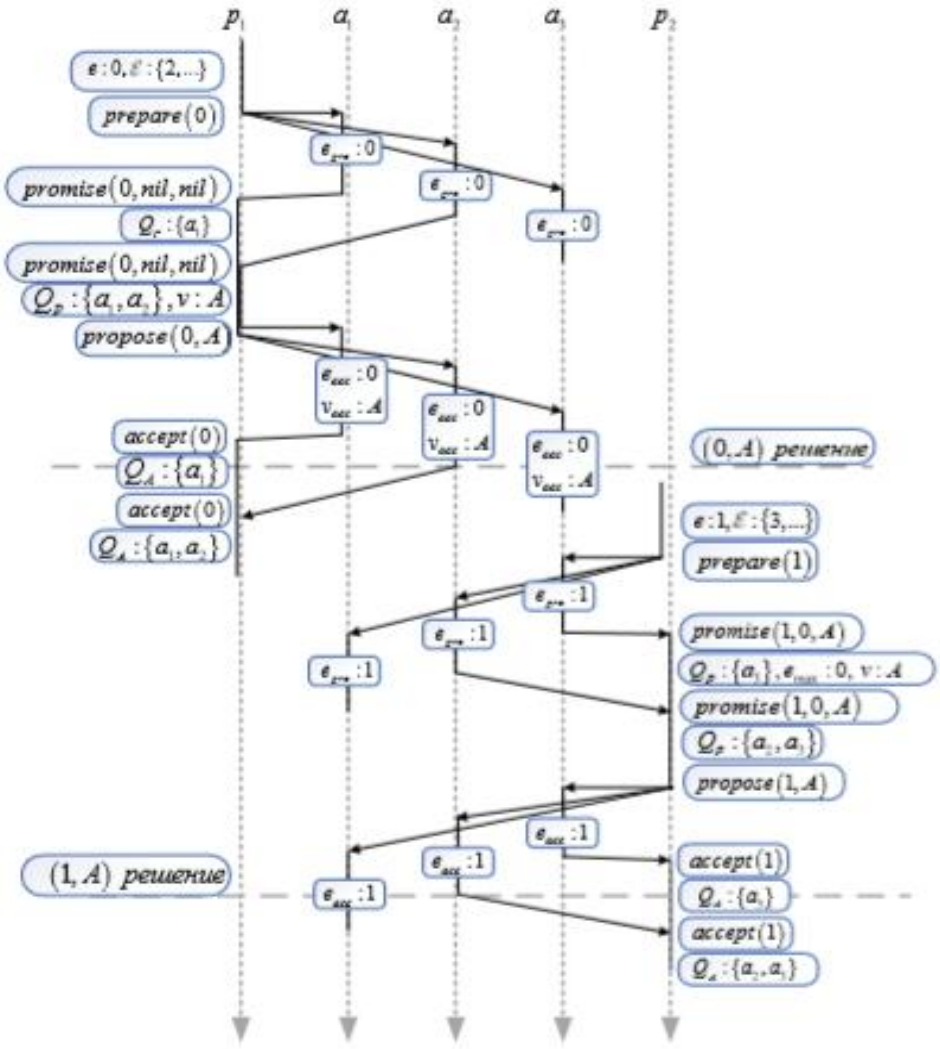


Рис. 1. Диаграмма исполнения алгоритма классического Паксоса для двух предлагающих, действующих последовательно

Свойства Классического Паксоса. Прежде чем перейти к доказательству надежности, сформулируем свойства классического Паксоса. Первые пять свойств относятся к алгоритму предлагающего, последующие пять – к алгоритму акцептора.

Свойство 1. Предлагающие используют уникальный номер раунда для каждого предложения.

Свойство 2. Предлагающие предлагают значение только после получения сообщений от $\left\lceil n_a / 2 \right\rceil + 1$ акцепторов.

Свойство 3. Предлагающие принимают значение только после того, как получают подтверждения от $\left\lceil n_a / 2 \right\rceil + 1$ акцепторов.

Свойство 4. Предлагающие обязаны выбрать значение для предложения в соответствии с правилами выбора значения. Если нет ранее принятых предложений, может быть выбрано любое значение. Если одно или более ранее предложенных значений было принято, выбирается значение с самым большим номером раунда.

Свойство 5. Каждый номер раунда, использованный предлагающим, должен быть больше, чем использованные прежде.

Свойство 6. Каждое сообщение, принятое акцептором, должно содержать номер раунда больший либо равный последнему принятому сообщению. Иначе такое сообщение не будет обработано.

Свойство 7. После каждого обработанного сообщения номер раунда принимается за тот, который содержало сообщение.

Свойство 8. Каждому сообщению $prepare(\ )$ должно быть отвечено сообщением $promise(\ )$.

Свойство 9. На каждое предложение акцептор отвечает после обновления последнего принятого предложения.

Свойство 10. Последний предложенный номер раунда и последнее принятое предложение неизменно и может быть только обновлено.

Доказательство надежности классического Паксоса. Для этого требуется показать, что если значение было согласовано, то никакое другое значение согласованным быть не может. Сначала сформулируем несколько лемм.

Лемма 1. Последний номер раунда, сохраненный каждым акцептором, может только монотонно возрастать.

Лемма 2. Последний номер раунда всегда больше либо равен последнему принятому номеру раунда для каждого из акцепторов.

Лемма 3. Для всех сообщений, отправленных акцепторами в форме $promise(e, f, v)$, где $f \neq nill$, верно что $e \geq f$.

Следствие 1. Все сообщения, которые отправлены предлагающими должны быть либо в форме $promise(e, nil, nil)$, либо в форме $promise(e, f, v)$, где $e > f$.

Следствие 2. Если предлагающий в раунде с номером e получает сообщение $promise(e, f, v)$, где $e = succ(f)$, значит в течение фазы предлагающий отправит значение v.

Лемма 4. Если значение v предложено в раунде с номером e, ни одно другое значение в этом раунде предложено быть не может.

Лемма 5. Если серия сообщений была отправлена акцептором, тогда сообщения частично упорядочены в том порядке, в котором они были отправлены. Это верно вне зависимости от типа сообщений.

Лемма 6. Если значение v согласовано в раунде с номером e, тогда как минимум один акцептор, который принял предложение (e, v), будет обязан отправить сообщение в будущих предложениях с большим номером раунда.

Доказательство леммы 6. Обе фазы классического Паксоса требуют участия большинства акцепторов (согласно свойству 2). Любые два большинства акцепторов будут пересекаться. Другими словами, они будут иметь как минимум одного общего акцептора.

Теорема 1. Если значение v согласовано в раунде с номером e и значение w предложено в раунде с номером f, так что $e < f$, то $v = w$.

Иными словами, теорема 1 определяет, что как только значение было согласовано в раунде с номером e, все последующие раунды, которые достигнут согласованного значения, достигнут его относительно того же значения.

Таким образом, чтобы доказать надежность в соответствии с вышеизложенными свойствами, с помощью вышеизложенных лемм, нам требуется показать следующее:

Теорема 2. Если значение v согласовано с номером раунда e, а значение w согласовано с номером раунда f, то $v = w$.

Данную теорему можно перефразировать следующим образом: если значение v было согласовано, то все номера раундов ограничены v.

Доказательство теоремы 2. В лемме 4 мы показали, что максимум одно значение будет предложено в любом из раундов. Так как необходимо чтобы значение было предложено прежде, чем оно будет согласовано, это значит, что как максимум одно значение может быть согласовано в одном раунде. Рассмотрим случай, где $e \neq f$. Так как номера раундов полностью упорядочены, то либо $e < f$, либо $e > f$. Так теорема 1 предполагает симметричность, то мы можем исключить $e > f$ из-за взаимозаменяемости указанных неравенств. Так как каждое согласованное значение сначала должно быть предложено, то более строгой теоремой является теорема 1.

Теперь докажем, что только согласованное значение может быть отправлено предлагающим.

Лемма 7. Если значение v отправлено предлагающим, то оно согласовано.

Доказательство леммы 7. Рассмотрим предлагающего p, который отправил значение v. Перед этим он получил сообщение $accept(e)$ от большинства акцепторов (по свойству 3). Как мы знаем сообщение $accept(e)$ должно было быть послано в ответ на $propose(e,v)$ от предлагающего p (по свойству 1). Таким образом, большинство акцепторов должно было принять предложение (e,v). Это значит, что, по определению, значение v было согласовано (по свойству 9).

2 Модификации алгоритма Паксос

Выше проанализирован алгоритм классический Паксос как единый алгоритм для решения проблемы распределенного консенсуса относительно одного значения. Однако, Паксос может рассматриваться как базис для построения разнообразных алгоритмов решения задачи распределенного консенсуса в виде модификаций классического Паксоса [10, 11].

Модификация «негативные ответы». Классический Паксос, как он был проанализирован до этого момента, может быть описан следующим образом: «если нет положительного ответа, ответа не должно быть никакого». Если быть точнее, акцепторы не ответят предлагающим, чей номер раунда e меньше, чем последнее их сообщение. Таким образом, мы будем выжидать пока истечет фиксированный период времени и отправлять новое сообщение с новым номером раунда (рис. 2).

Такое поведение может быть улучшено добавлением негативных ответов, таких как $no-promise(e)$ и $no-accept(e)$. Такие отрицательные сообщения будут отправлены акцепторами принимающим, в случае получения сообщений, в которых $e < e_{pro}$. Когда предлагающий получает отрицательное сообщение, он может сразу отправить предложение с большим числом раунда. Кроме того, он может проигнорировать сообщение и подождать ответа от большинства участников. Если предлагающий получает отрицательное сообщение от большинства, то его предложение отклоняется и требуется передача нового предложения. Для предлагающего безопасно прекратить выполнение либо начать его заново с любой стадии, так как это будет эквивалентно нормальному поведению (ожидание и новая попытка).

Акцепторы могут добавлять информацию в отрицательные ответы, такую как номер раунда f, например $no-promise(e,f)$ и $no-accept(e,f)$. Или же (g,v), то есть последнее принятое акцептором предложение, например $no-promise(e,f,g,v)$, $no-accept(e,f,g,v)$.

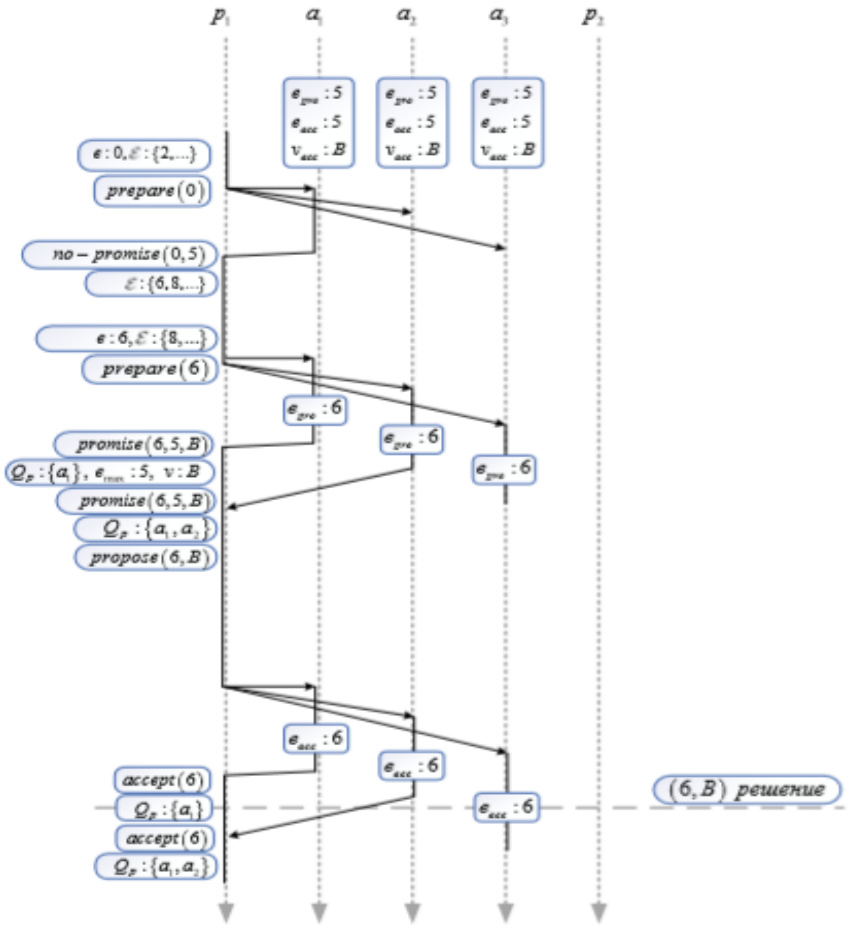


Рис. 2. Диаграмма исполнения Паксоса с негативными ответами

Обход второй фазы. Может быть показано, что алгоритм предлагающего для классического Паксоса, строго говоря, делает больше работы, чем необходимо для выполнения требований распределенного консенсуса. На практике, если предлагающий узнает, что значение было уже согласовано, так как большинство акцепторов вернули одно и то же предложение во время первой фазы, то предлагающий может не начинать вторую фазу, а принять значение. Таким образом, существует три возможных случая для завершения первой фазы предлагающим:

1) Решение не было принято. Ни одно предложение не сопровождалось сообщением вида $promise(\ )$ во время первой фазы, то есть значение не было пока согласовано. Предлагающий отправит значение-кандидат во второй фазе.

2) Решение принято. Значение было согласовано и согласовано, предлагающий принял значение. Никаких дополнительных действий не требуется.

3) Неопределенность. Некоторые предложения были возвращены в первой фазе. Предлагающим не определено, достигнута ли точка заключения соглашения. Если она была достигнута, согласованное значение – это значение, пришедшее с самым большим номером раунда.

Предлагается повысить вероятность обхода второй фазы (рис. 3), используя следующий подход:

1) Если предлагающий получил довольно много одинаковых сообщений в первой фазе, но не достиг $\left[n_a / 2 \right] + 1$, он может ждать доставки большего количество сообщений.

2) Потребуется выставление ограничения на этот период ожидания, чтобы гарантировать прогресс.

3) Предлагающий может одновременно начать вторую фазу, но продолжить ожидание сообщений первой фазы. Если необходимое количество сообщений было получено до того, как вторая фаза завершена, оставшуюся часть второй фазы можно пропустить.

4) Предлагающий может отслеживать не только возвращенные предложения с самым большим номером раунда, а все возвращенные предложения.

5) Предлагающие могут использовать сообщения по новой с предыдущими номерами раундов, не прерывая процесс наблюдения. Это потребует сохранения всех полученных предложений.

6) Предлагающие могут использовать негативные ответы.

7) Акцепторы могут хранить все принятые предложения, а не только последнее. Акцепторы могут затем отправлять предложения и негативные ответы для предоставления предлагающим более исчерпывающий информации о статусе, в котором находится система.

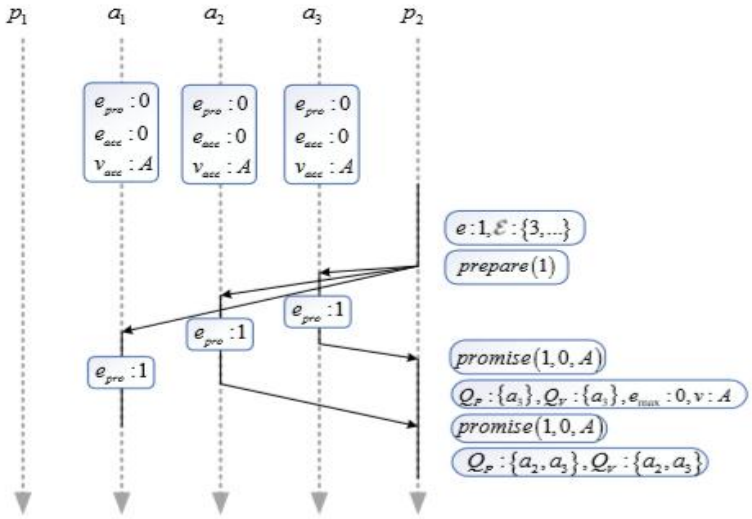


Рис. 3. Диаграмма исполнения Паксоса с обходом второй фазы

Мульти-Паксос. До этого момента мы рассматривали проблему достижения консенсуса относительно одного значения. На практике, такие алгоритмы чаще всего используются для достижения соглашения относительно бесконечной последовательности значений. Мы можем разделить существующие алгоритмы на два подкласса:

1) Классический Паксос, алгоритмы которого основаны на идее множества участников, которые договариваются об одном значении. Примерами могут послужить собственно известные классический Паксос, быстрый Паксос, *Mencius*. Такие подходы редко используются в промышленных системах.

2) Алгоритмы мульти-Паксос основаны на идее роли лидера, который выполняет первую фазу над последовательностью, а затем координирует процесс принятия решения пока эту роль не получит новый лидер. Такой подход широко используется на практике, а примерами могут послужить *Chubby*, *Zookeeper*, *Raft*.

Ключевое преимущество мульти-Паксоса в том, что в стабильном состоянии каждое решение достигается за один раунд приема-передачи от большинства акцепторов и одну синхронную запись. Система стабильна, если существует только один предлагающий (лидер), он во второй фазе и большинство акцепторов отвечают и «живы». Система должна находиться в таком состоянии большую часть времени.

Мульти-Паксос перекладывает довольно ощутимую «ответственность» на лидера. В стабильном состоянии этот предлагающий несет ответственность за получение значения-кандидата, нумерацию индексов, предложение значений акцепторам, сбор принятых значений, получение согласованных значений и отправку сообщений участникам о принятых решениях. Из-за этого, лидер часто является так называемым бутылочным горлышком всей

системы. Такой несбалансированный подход ведет к перегруженности лидера и его сетевых соединений, пока другие участники недонагружены. Более того, необходимость передавать значения-кандидаты лидеру вносит дополнительную отправку сообщений и лишний раунд приема-передачи. Всё это отражает существенные недостатки модификации мульти-Паксос.

Выводы

Показано, что алгоритм классического Паксоса более строг, чем необходимо. В частности, требование по пересечению кворума (которое накладывает жёсткое условие, чтобы все кворумы пересекались) может быть значительно ослаблено. Такое ослабление позволяет значительно повысить гибкость метода достижения распределенного консенсуса и его надёжность в реальных условиях, а главное, в условиях, близких или соответствующих режиму отказа системы, где алгоритм классического Паксоса не обеспечивает консенсуса.

Дальнейшие исследования требуют разработки экспериментального окружения для моделирования системы с заданными параметрами и экспериментальной проверки производительности и надёжности классического и предложенного методов.

Литература

1. Биденко С.И., Якушев Д.И. Геоинформационные управляющие системы и технологии: Монография. – СПб: Изд-во СПбУ МВД, 2014. – 248 с.

2. Черный С.Г., Николашин Ю.Л., Присяжнюк А.С., Миляков Д.Ф., Биденко С.И. Расширение геолокационного функционала ГНСС сервисами мобильной сетевой ASSIST-поддержки в интересах моделирования (освещения) территориальной обстановки // Информация и Космос. 2020. № 2. С. 118 – 123.

3. Distributed consensus revised [Электронный ресурс]. Режим доступа: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-935.pdf.

4. Generalized Consensus and Paxos [Электронный ресурс]. Режим доступа: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2005-33.pdf.

5. Жиленков А.А., Черный С.Г. Повышение эффективности систем автоматического управления автономными буровыми установками за счет разработки методов обеспечения их совместимости и интеграции // Автоматизация, телемеханизация и связь в нефтяной промышленности. 2015. № 4. С. 9-18.

6. Zhilenkov A.A., Gilyazov D.D., Matveev I.I., Krishtal Y.V. Power line communication in iot-systems. Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, ElConRus 2017 - 2017. Pp. 242-245.

7. Zhang Y., Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems. IFAC Symposium Fault Detection Supervision and Safety of Technical Processes, SAFEPROCESS (Washington, D.C., USA, 2003). Pp. 265–276.

8. Qu Z., Ihlefeld C.M., Yufang J., Saengdeejing A. Robust fault-tolerant self-recovering control of nonlinear uncertain systems. Automatica. 2003. 39(10). Pp. 1763–1771.

9. Richter J.H., Weiland S., Heemels W., Lunze J. Decoupling-based reconfigurable control of linear systems after actuator faults. 10th European Control Conference, ECC (Budapest, Hungary, 2009). Pp. 2512–2517.

10. Nobrega, E.G., Abdalla M.O., Grigoriadis K.M. Robust fault estimation of unceratain systems using an LMI-based approach. Int. J. Robust Nonlinear Control. 2008. 18(7). Pp. 1657–1680.

11. Witczak, M. Modelling and Estimation Strategies for Fault Diagnosis of Non-linear Systems. – Springer-Verlag, Berlin. 2007. 212 p.

References

1. Bidenko S.I., Yakushev D.I. *Geoinformacionnye upravlyayushchie sistemy i tekhnologii* [Geoinformation control systems and technologies]: Monografiya. – SPb: SPbU MVD, 2014. – 248 s. (in Russian).

2. Black S.G., Nikolashin Yu.L., Jury A.S., Milyakov D.F., Bidenko S.I. *Rasshirenie geolokacionnogo funkcionala GNSS servisami mobil'noj setevoj ASSIST-podderzhki v interesah modelirovaniya (osveshcheniya) territorial'noj obstanovki* [Extension of GNSS geolocation functionality with mobile network ASSIST support services for modeling (lighting) of territorial situation]. Information and Space. 2020. No 2. Pp. 118 – 123 (in Russian).

3. Distributed consensus revised [Электронный ресурс]. Режим доступа: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-935.pdf.

4. Generalized Consensus and Paxos [Электронный ресурс]. Режим доступа: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2005-33.pdf.

5. Zhilenkov A.A., Black S.G. *Povyshenie effektivnosti sistem avtomaticheskogo upravleniya avtonomnymi burovymi ustanovkami za schet razrabotki metodov obespecheniya ih sovmestimosti i integracii* [Improving the efficiency of automatic control systems of autonomous drilling rigs by developing methods for ensuring their

compatibility and integration]. Automation, telemechanization and communication in the oil industry. 2015. No 4. Pp. 9-18. (in Russian).

6. Zhilenkov A.A., Gilyazov D.D., Matveev I.I., Krishtal Y.V. Power line communication in iot-systems. Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, ElConRus 2017 - 2017. Pp. 242-245.

7. Zhang Y., Jiang J. Bibliographical review on reconfigurable fault-tolerant control systems. IFAC Symposium Fault Detection Supervision and Safety of Technical Processes, SAFEPROCESS (Washington, D.C., USA, 2003). Pp. 265–276.

8. Qu Z., Ihlefeld C.M., Yufang J., Saengdeejing A. Robust fault-tolerant self-recovering control of nonlinear uncertain systems. Automatica. 2003. 39(10). Pp. 1763–1771.

9. Richter J.H., Weiland S., Heemels W., Lunze J. Decoupling-based reconfigurable control of linear systems after actuator faults. 10th European Control Conference, ECC (Budapest, Hungary, 2009). Pp. 2512–2517.

10. Nobrega, E.G., Abdalla M.O., Grigoriadis K.M. Robust fault estimation of unceratain systems using an LMI-based approach. Int. J. Robust Nonlinear Control. 2008. 18(7). Pp. 1657–1680.

11. Witczak, M. Modelling and Estimation Strategies for Fault Diagnosis of Non-linear Systems. – Springer-Verlag, Berlin. 2007. 212 p.

Статья поступила 16 сентября 2020 г.

Информация об авторах

Черный Сергей Григорьевич – Кандидат технический наук, доцент. Заведующий кафедрой «Информационные технологии» ФГБОУ ВО «Керченский государственный морской технологический университет». Тел. (36561) 6-35-85. E-mail: sergiiblack@gmail.com.

Адрес: 298309, Республика Крым, г. Керчь, ул. Орджоникидзе, д. 82.

Биденко Сергей Иванович – Доктор технических наук, профессор. Советник генерального конструктора ПАО «Интелтех». Тел. +7 (812) 363-19-29. E-mail: BidenkoSI@inteltech.ru.

Адрес:197342, Россия, Санкт-Петербург, ул. Кантемировская, д. 8.

Якушев Денис Игоревич – Профессор кафедры специальных информационных технологий ФГКОУ ВО «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации», доктор технический наук. Тел. +7 (812 744-70-00). E-mail: yakushev@pisem.net.

Адрес: 198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1.

The existence and achievability of consensus as a problem of ensuring reliability in distributed geo-cybernetic platforms

S.G. Black, S.I. Bidenko, D.I. Yakushev

Annotation. *The problem of achieving consensus today has become one of the cornerstones in building reliable distributed (especially cloud and blockchain) applications and cyber-physical systems. Local services, as well as the whole paradigm of building monolithic applications, are significantly outdated and are no longer able to provide the reliability parameters required by modern systems. The article considers the problem of reaching consensus using the example of the Paxos family of algorithms. The results of the analysis of the properties of individual algorithms, the analysis of strengths and weaknesses in various approaches to the improvement of the classical Paxos algorithm are presented. The reliability of the consensus algorithm is proved.*

Keywords: *reliability; cyberphysical system; control; distributed system.*

Information about Authors

Black Sergey Grigoryevich – Ph.D., Associate Professor. The head of the Department of Information Technologies of the Kerch State Maritime Technology University. Tel. (36561) 6-35-85. E-mail: sergiiblack@gmail.com. Address: 298309, Republic of Crimea, Kerch, Ordzhonikidze St., 82.

Bidenko Sergey Ivanovich – Ph.D., Professor. Advisor to general designer Inteltech. Tel. 7 (812) 363-19-29. E-mail: BidenkoSI@inteltech.ru. Address: 197342, Russia, St. Petersburg, Kantemirovsky St., 8.

Yakushev Denis Igorevich – Professor of Special Information Technology Department of the Federal University of the Russia Federation Ministry Interior. Tel.: 7 (812) 744-70-00. E-mail: yakushev@pisem.net.

Address: 198206, St. Petersburg, St. Petersburg, St. Petersburg, 1.

Для цитирования: Черный С.Г., Биденко С.И., Якушев Д.И. Существование и достижимость консенсуса, как проблема обеспечения надёжности в распределённых геокибернетических платформах // Техника средств связи. 2020. № 3 (151). С. 69-79.

For citation: Black S.G., Bidenko S.I., Yakushev D.I. The existence and achievability of consensus as a problem of ensuring reliability in distributed geo-cybernetic platforms. Means of communication equipment. 2020. No 3 (151). Pp. 69-79 (in Russian).

УДК 65-011-56

Критерий размерности множеств альтернатив в экспертных оценках, проводимых методом парных сравнений

Севастьянов С.И.

Аннотация. *В статье разрешается* ***проблема*** *выбора и формализации критерия размерности множеств альтернатив в экспертных оценках, проводимых методом парных сравнений.* ***Целью работы*** *является разработка математического аппарата, позволяющего определять количественные значения критерия размерности множеств альтернатив.* ***Новизна:*** *разработана система критериев размерности для малых, средних и больших множеств альтернатив. Выявлена вторая особенность парных сравнений, связанная с введенными понятиями «цикла парных сравнений» и «нижней и верхней границами цикла парных сравнений».* ***Результат:*** *формализованы исходные данные метода парных сравнений, приведены их определения. Формализованы особенности метода парных сравнений, выраженные в функциональной зависимости количества учитываемых альтернатив в экспертных оценках и количества сравниваемых альтернатив, которые упорядочивают, из состава учитываемых альтернатив, в блоки (матрицы) парных сравнений. Разработаны принципы упорядочения альтернатив и выражения расчетов значений критерия размерности, проработанного в качестве системы критериев размерности для малых, средних и больших множеств альтернатив. Первая и вторая особенности парных сравнений иллюстрированы примерами. Представлены расчеты количественных значений критериев размерности для малых, средних и больших множеств альтернатив, а также верхних и нижних границ циклов парных сравнений, исходя из выбираемого значения, от четырех до семи альтернатив, критерия психологического ограничения эксперта.* ***Выводы:*** *разработан математический аппарат, позволяющий определять количественные значения критерия размерности множеств альтернатив в экспертных оценках, проводимых методом парных сравнений.* ***Практическая значимость*** *заключается в том, что разработанный математический аппарат дает возможность не только теоретически обосновывать выбор и рассчитывать количественные значения критериев размерности множеств альтернатив для различных аспектов экспертных оценок, но и проводить экспертные оценки со множествами, которые по своей мощности могут намного превышать множества альтернатив, рассмотренных в статье.*

Ключевые слова: *экспертная оценка, критерий психологического ограничения эксперта; методы и особенности парных сравнений; малые, средние и большие множества альтернатив; критерий размерности; цикл парных сравнений; нижняя и верхняя границы цикла парных сравнений.*

Введение

Парные сравнения [1] приобретают все большее значение, по мере распространения экспертных методов. Они лежат в основе многих методов упорядочения альтернатив. Вместе с тем, анализ литературы, посвященной экспертным парным сравнениям альтернатив, не дал определенного ответа, что понимается под количественными значениями критерия размерности множеств альтернатив для малых, средних и больших множеств альтернатив, хотя ссылки на малое число [2], большое число альтернатив [2, 3], широкий класс объектов [3], значительное количество учитываемых свойств [4] используются достаточно широко. Необходимость точного категорирования терминов, касающихся объемов множеств альтернатив, в ряде экспертных задач, и потребность в наглядном примере, в части расчетов количественных значений критерия размерности множеств альтернатив для малых, средних и больших множеств альтернатив, определяет актуальность статьи.

В ряде работ, рекомендуется количество альтернатив в экспертных оценках не превышать более: семи в [4-6]; девяти [3]; десяти [2]; двенадцати [7]; пятнадцати [8]. Рациональным количеством альтернатив, например, при применении метода расстановки приоритетов [2], считается 6, а для метода анализа иерархий – 7. В работе [2] под малым числом объектов в экспертных оценках, методом парных сравнений понимается количество

объектов, равное 4-6, в работе [3] допускаются количественные значения критерия размерности множеств альтернатив, равные 7 ± 2.

Все перечисленные рекомендации имеют ограничение сверху, которое, в той или иной степени, связанно с количественным значением критерия, определяющего психологическое ограничение эксперта, проводящего парные сравнения. Широко известно, что таковым является число семь [4-6]. В экспертных оценках при количестве альтернатив более семи могут иметь место грубые ошибки экспертов. Возможно, этот уровень количественного значения критерия психологического ограничения эксперта можно принять за количественное значение критерия размерности множеств альтернатив, разбивающего множество альтернатив на малые и средние, или малые и большие. Но как показывает анализ литературы, посвященной данному вопросу, и практика сравнительного анализа – критерий психологического ограничения эксперта применяется в качестве критерия размерности множества альтернатив далеко не всегда. Одним из объяснений этому является то, что критерий-константа не адекватен всем аспектам задач упорядочения альтернатив. На практике более приемлемым оказывается гибкий критерий (система критериев), динамика изменений количественного значения которого соответствует разнообразию аспектов задач упорядочения альтернатив в экспертных оценках, проводимых методом парных сравнений. Реализация данного подхода требует разработки соответствующего математического аппарата.

В связи с этим, целью статьи является разработка математического аппарата, позволяющего в экспертных оценках, проводимых методом парных сравнений, определять количественные значения критерия размерности множеств альтернатив для малых, средних и больших множеств. Также актуально рассмотрение вопросов практической применимости полученных научных результатов.

Первая особенность метода парных сравнений. Формализация исходных данных, определение терминов, пример

Наиболее известными и апробированными методами решения экспертных задач, в основе которых лежат парные сравнения, являются методы анализа иерархий и расстановки приоритетов [9]. Для упорядочения множеств с большим числом альтернатив в работе [2] приводится блочный метод решения задачи расстановки приоритетов, а в [3] – метод иерархической декомпозиции. В этих работах учитываемые альтернативы группируются (в качестве первой оценки) в сравниваемые блоки или «классы» (в дальнейшем будем использовать термин блоки) из шести или семи альтернатив в каждом, а каждый очередной блок альтернатив включает альтернативы с большими весами, в отличие от весов альтернатив предыдущего блока. Особенностью методов является то, что при этом альтернатива с наивысшим весом в блоке также включается в следующий блок с большими весами и как своеобразный стержень между двумя блоками придает однородность шкале оценок [3]. Вошедшие в блоки альтернативы, определенным образом обрабатываются в квадратных матрицах парных сравнений, количество которых равно количеству сравниваемых блоков: порядок этих матриц равен количеству альтернатив в этих блоках.

Особенности парных сравнений для большого числа альтернатив в формализованном виде в рассматриваемой литературе не приведены или имеют описательный характер. Тогда как для определения количественных значений критерия размерности множеств альтернатив в парных сравнениях эта формализация необходима. С этой целью в настоящей статье формализованы исходные данные метода парных сравнений для больших множеств, и приведены их определения в следующем виде:

a – учитываемая альтернатива. Это альтернатива, принятая к учету при постановке задачи упорядочения альтернатив;

a^* – сравниваемая альтернатива. Это альтернатива, из состава учитываемых альтернатив, упорядоченная методом парных сравнений в блоки (матрицы) парных сравнений;

A_R – конечное множество учитываемых альтернатив $A_R = \{a_r \in A_R / r = \overline{1, R}\}$, $card\ A_R = R$, где

R – мощность множества A_R или количество учитываемых альтернатив, принятых к упорядочению перед их разбиением на «сравниваемые блоки» [2, 3];

b_z – учитываемый полный блок, в котором количество учитываемых альтернатив, входящих в него, равно – r^b (r^b = const), $b_z \in B$;

B – множество учитываемых полных блоков, $B = \{b_Z \in B / z = \overline{1, Z}\}$;

Z – мощность множества B или количество учитываемых полных блоков во множестве A_R.

Под полным блоком будем понимать блок из множества блоков, на которые разбивается количество учитываемых альтернатив (R) или количество сравниваемых альтернатив (R^*), в котором количество альтернатив равно r^b.

r^b – количество учитываемых или сравниваемых альтернатив в соответствующих полных блоках, равное константе (r^b = const).

Множество A_z – собственное подмножество множества A_R, где $A_R = \{A_z \in A_R / z = \overline{0,(Z+1)}\}$. Подмножество A_z включает в себя учитываемые альтернативы, которые составляют учитываемые блоки. Если $z = \overline{1,Z}$, то A_z содержит в себе полный блок. Подмножество A_z может включать в себя альтернативы количеством, меньшим чем r^b (неполные блоки), если $z = (0 \vee (Z+1)$.

Под учитываемым неполным блоком будем понимать блок, в котором число учитываемых альтернатив меньше r^b и равно учитываемому остатку (r^{ob}), где r^{ob} – учитываемый остаток альтернатив, который равен количеству учитываемых альтернатив в неполном блоке, то есть мощности подмножества A_z, если $z = 0 \vee (Z+1)$.

При проведении парных сравнений в последнем блоке возможен остаток как для учитываемых, так и для сравниваемых альтернатив в случае, если R или R^* не кратно r^b, а также остаток может быть в первом блоке, который одновременно является и последним блоком, при $z = 0$ и $R < r^b$.

Количество учитываемых полных блоков (Z) вычисляется путем деления количества учитываемых альтернатив (R) на количество альтернатив в полном блоке (r^b), согласно выражению (1):

$$Z =]\, R / r^b\, [\qquad (1)$$

где знак] [означает целую часть числа.

При этом,

$$\begin{cases} \text{если } R \text{ – кратно } r^b, \text{ то } R = Z\, r^b, \\ \text{если } R \text{ – не кратно } r^b, \text{ то } R = Z\, r^b + r^{ob}. \end{cases} \qquad (2)$$

Разница между учитываемыми и сравниваемыми альтернативами, множествами, подмножествами, остатками, полными и неполными блоками вносится особенностью парных сравнений, отмеченной в работах [2, 3].

Для сравниваемых альтернатив, в отличие от учитываемых, справедливо следующее:

A^*_R – конечное множество сравниваемых альтернатив в парных сравнениях,

$$A^*_R = \{a^*_r \in A^*_R |\ r = \overline{1, R^*}\},\ card\ A^*_R = R^*,$$

где R^* – мощность множества сравниваемых альтернатив или количество сравниваемых альтернатив, получаемое в путем учета в R^* дважды одной и той же учитываемой альтернативы – a_r ($r = \overline{1, R}$), которую таким образом включают в смежные сравниваемые

полные блоки (b^*). При этом в ряду сравниваемых альтернатив эта учитываемая альтернатива (a_r) на стыке смежных блоков числится как две сравниваемые альтернативы, но с разными индексами – a^*_r и a^*_{r+1}, где $r = \overline{1, R^*}$;

b^* – сравниваемый полный блок, в котором количество альтернатив, входящих в него, также равно – r^b (r^b = const), $b^* \in B^*$;

B^* – множество сравниваемых полных блоков, $B^* = \{b^*_Z \in B^* \mid z = \overline{1, Z}^*\}$;

Z^* – мощность множества B^* или количество сравниваемых полных блоков во множестве A^*_R.

Множество A^*_z – собственное подмножество множества A^*_R,
где $A^*_R = \{A^*_z \in A^*_R \mid z = \overline{0, (Z^*+1)}\}$.

A^*_z включает в себя сравниваемые альтернативы, которые составляют z-ый сравниваемый полный блок – b^*_Z, если $z = \overline{1, Z}^*$, или неполный блок, если $z = 0 \vee (Z^*+1)$;

r^{ob*} – сравниваемый остаток альтернатив, который равен количеству сравниваемых альтернатив в сравниваемом неполном блоке или мощности подмножества A^*_z, если $z = 0 \vee (Z^*+1)$;

Количество сравниваемых полных блоков (Z^*) вычисляется путем деления количества сравниваемых альтернатив (R^*) на количество альтернатив в полном блоке (r^b) согласно выражению (3):

$$Z^* =] R^* / r^b [. \quad (3)$$

При этом,

$$\begin{cases} \text{если } R^* \text{ – кратно } r^b, \text{ то } R^* = Z^* r^b, \\ \text{если } R^* \text{ – не кратно } r^b, \text{ то } R^* = Z^* r^b + r^{ob*}. \end{cases} \quad (4)$$

В отличие от учитываемых альтернатив, матрицы парных сравнений формируются методом парных сравнений только для сравниваемых альтернатив.

Порядок матриц парных сравнений равен количеству альтернатив в полном блоке (r^b), а для неполных блоков – r^{ob*}. При этом в матрицах учитывается только $r^{ob*} \geq 2$. Поскольку ситуация когда, $r^{ob*} = 1$ означает, что из предыдущего смежного полного блока, согласно вышеуказанной особенности парных сравнений, в последующий неполный блок второй раз вносится и учитывается наибольшая альтернатива предыдущего блока. В этом случае данная процедура не имеет смысла – парные сравнения с одной и той же альтернативой не проводятся по определению.

Количество сравниваемых альтернатив в парных сравнениях (R^*), с учетом особенности парных сравнений, определяется через R согласно выражению (5):

$$R^* = \{(R + Z \mid r^{ob} \neq 0) \vee ((R + (Z - 1) \mid r^{ob} = 0)\}, \quad (5)$$

где R – количество учитываемых альтернатив множества A_R;

Z – количество учитываемых полных блоков множества A_R;

r^{ob} – учитываемый остаток альтернатив.

Приведенные выражения можно проиллюстрировать на примере 1 (рис. 1), в котором в соответствии с выражениями (1), (3), (5) для $r^b = 4$ показана первая особенность парных сравнений, выраженная в зависимости Z, a^*_r, Z^*, R^* от выбираемого количества учитываемых альтернатив R и количества альтернатив в полном блоке – r^b.

В приведенном примере 1, в строке А) – «R (a_r)», рассмотрим количество учитываемых альтернатив (например, $R = \overline{1,48}$), которое разбивается на учитываемые полные блоки ($Z = \overline{0,12}$) по четыре альтернативы ($r^b = 4$) в каждом полном блоке. Альтернативы, выделенные жирным шрифтом – наибольшие по весу в соответствующем учитываемом полном блоке альтернатив. В строке Е) – «Z» показаны соответствующее $R(a_r)$ количество учитываемых полных блоков (от 0 до 12 для $R = \overline{1,48}$).

В строке Б) – «a_r в блоках Z^*» показана первая особенность парных сравнений, когда одна и та же альтернатива a_r^* (жирный шрифт), на стыке блоков, включается дважды, соединяя в одну шкалу смежные сравниваемые полные блоки.

В строке В) – «$R^*(a^*_r)$» показана динамика изменения количества сравниваемых альтернатив R^* (R^*=$\overline{1,59}$) относительно учитываемых альтернатив R ($R = \overline{1,48}$).

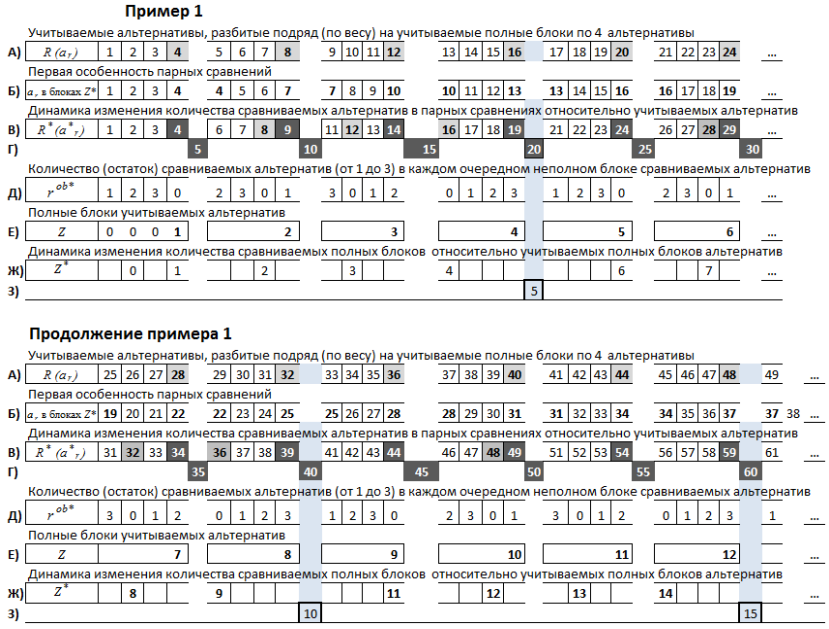


Рис. 1. Пример 1 учитываемых альтернатив

В строке Ж) – показана динамика изменения количества сравниваемых полных блоков «Z^*» относительно учитываемых полных блоков «Z», а в строке Д) – количество (остаток – r^{ob*}) сравниваемых альтернатив (от 1 до 3) в каждом очередном неполном блоке альтернатив.

Количества сравниваемых альтернатив в строках В) и Г), выделенные на черном фоне жирным белым шрифтом и связанные в этих строках по диагонали (между смежными блоками), образованы в результате двойного учета (с разными индексами) одной и той же сравниваемой альтернативы (первая особенность парных сравнений).

В строке З) для $r^b = 4$ показано формирование дополнительных «пятых» (5, 10, 15 …) сравниваемых полных блоков, получаемых в результате вышеприведенной первой особенности парных сравнений (двойного учета одной и той же альтернативы на стыке блоков).

Таким образом, приведенный пример 1 показывает первую особенность парных сравнений, выраженную в функциональной зависимости количества R^* (a^*_r) относительно количества $R(a_r)$, и соответствующую динамику количественных изменений R и R^*, Z и Z^*.

Вторая особенность метод парных сравнений. Формализация исходных данных, определение терминов

В ходе формализации исходных данных методом парных сравнений для больших множеств выявлена вторая его особенность, связанная с циклами парных сравнений (v).

Под циклом парных сравнений (v) понимается последовательный ряд из учитываемых или сравниваемых полных блоков, количество которых равно r^b. Цикл имеет нижнюю границу цикла парных сравнений и верхнюю границу цикла парных сравнений. Количество альтернатив (r^v) в цикле v, при $v = \overline{1,V}$ определяется согласно выражению (6)

$$r^v = (r^b)^2,\ r^v = \text{const}. \qquad (6)$$

Так, в примере 1 количество альтернатив в циклах v равно 16 ($r^v = (r^b)^2 = 16$).

Под нижней границей цикла парных сравнений понимается первая наименьшая по весу учитываемая ($a_r{}^{инг}$) или сравниваемая ($a_r{}^{*инг}$) альтернатива (количество альтернатив $R^{инг}{}_{\nu}$ и $R^{*инг}{}_{\nu}$) в цикле, начиная соответственно с первого полного блока цикла парных сравнений.

Под верхней границей цикла парных сравнений понимается последняя наибольшая по весу учитываемая ($a_r{}^{ивг}$) или сравниваемая ($a_r{}^{*ивг}$) альтернатива (количество альтернатив $R^{ивг}{}_{\nu}$ и $R^{*ивг}{}_{\nu}$) в цикле, соответственно последнего полного блока цикла парных сравнений и, при которой для $\nu = 1$ разница между количеством сравниваемых и учитываемых альтернатив ($\Delta^{\nu}{}_{R}$) равна r^b ($\Delta^{1}{}_{R} = R^* - R = r^b$), где $Z^*{}_1 - Z_1 = 1$, или кратно r^b при $\nu > 1$, так что $\Delta^{\nu}{}_{R}$ вычисляется по выражению (7)

$$\Delta^{\nu}{}_{R} = \nu r^b,\ \nu = \overline{1,V}, \tag{7}$$

где ν – количество циклов парных сравнений.

При этом ν рассчитывается по выражению (8):

$$\nu = Z^*{}_{\nu} - Z_{\nu}, \text{ при } r^{ob} = r^{ob*}. \tag{8}$$

Например, для $\nu = 2,3...V$, $\Delta^{\nu}{}_{R}$ будет соответственно равно $2r^b$, $3r^b$,..., Vr^b.

Количество учитываемых или сравниваемых полных блоков парных сравнений и количество альтернатив нижних и верхних границ в ν-х циклах парных сравнений вычисляются по выражениям (9) – (12):

$$Z_{\nu} = \nu\, r^b + 1, \tag{9}$$

где $\nu = \overline{1,V}$ – количество полных циклов;

r^b – количество полных блоков в цикле (равное количеству альтернатив в полном блоке).

$$Z^*{}_{\nu} = Z_{\nu} + \nu = \nu\, r^b + 1 + \nu = \nu\,(r^b + 1) + 1. \tag{10}$$

Для первого учитываемого или сравниваемого полного блока ($z = z^* = 1$; $\nu = 0$), после которого начинается отсчет циклов парных сравнений, справедливо $R = R^*$.

Для нижних и верхних границ полного цикла при $\nu > 0$ количество учитываемых и сравниваемых альтернатив вычисляется по выражениям (11) и (12):

$$\begin{cases} R^{инг}{}_{\nu} = r^b\,(\nu\, r^b + 1) + 1, \\ R^{ивг}{}_{\nu} = r^b\,(\nu\, r^b + 1). \end{cases} \tag{11}$$

$$\begin{cases} R^{*инг}{}_{\nu} = r^b\,(\nu\, r^b + \nu + 1) + 2, \\ R^{*ивг}{}_{\nu} = r^b\,(\nu\, r^b + \nu + 1). \end{cases} \tag{12}$$

Вторую особенность парных сравнений, являющейся следствием первой (5) и приведенную в выражениях (6) – (12), можно рассмотреть на примере 2, для $r^b = 4$.

Строки А) и В) примера 2 (рис. 2) соответствуют строкам А) и В) примера 1.

Для более наглядного представления циклов парных сравнений альтернатив, в примере 2 увеличено количество учитываемых альтернатив ($R = \overline{1,52}$), которое разбивается на учитываемые полные блоки ($Z = \overline{0,13}$) по четыре альтернативы ($r^b = 4$) в каждом полном блоке.

В строках Б) и Г) наглядно изображены три цикла парных сравнений для ν и ν*, а также количество альтернатив в циклах ν и ν*. Согласно выражений (7) и (8) $\Delta^{\nu}{}_{R} = 4, 8, 12$ и соответственно равна первому, второму и третьему циклам, при заданном $r^b = 4$.

В примере 2 изображены границы циклов $a_r{}^{инг}$, $a_r{}^{*инг}$ и $a_r{}^{ивг}$, $a_r{}^{*ивг}$, которые определяют начало и конец первого, второго и третьего циклов.

В целом, приведенные примеры 1 и 2 достаточно наглядно иллюстрируют первую и вторую особенности метода парных сравнений и позволяют проверить правильность формализованных выражений (1) – (12).

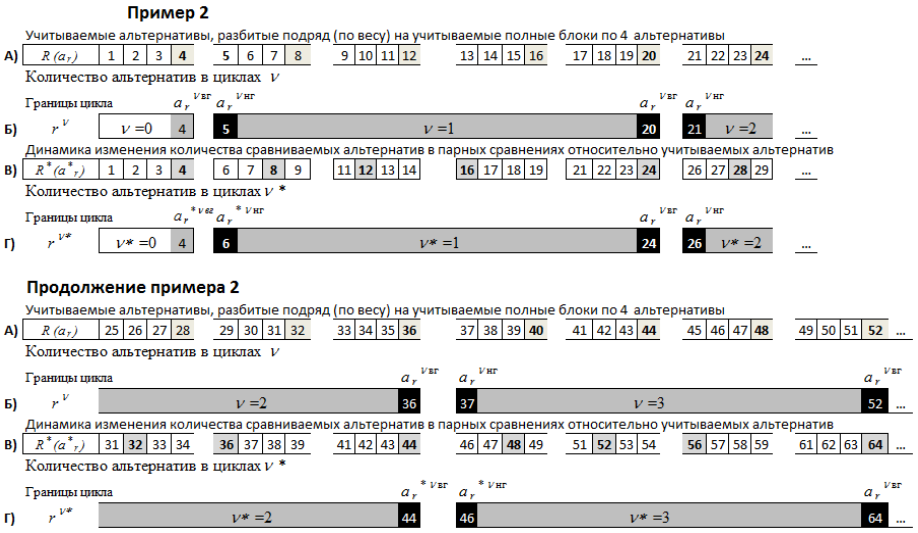


Рис. 2. Пример 2 учитываемых альтернатив

Физический смысл второй особенности парных сравнений, приведенных выражений (9) – (12), состоит в том, что в конце каждого очередного цикла парных сравнений, для последнего в данном цикле полного блока, количество учитываемых полных блоков (Z) продолжает монотонно увеличиваться на единицу, тогда как в количестве сравниваемых полных блоков (Z^*) происходит «скачок», оно увеличивается на две единицы, и далее продолжает монотонно увеличиваться на единицу – до начала следующего цикла (до очередного скачка).

Формализация исходных данных, определение терминов, первой и второй особенностей метода парных сравнений позволяет выявить функциональные зависимости между исходными данными метода парных сравнений и перейти к определению критерия размерности альтернатив. Выражения (1) – (12) являются основой разработанного математического аппарата, предназначенного для определения критерия (критериев) размерности малых, средних и больших множеств альтернатив в экспертных оценках, проводимых методом парных сравнений.

Принципы упорядочения альтернатив

Анализ особенностей метода парных сравнений позволяет перейти к частным задачам: разработке принципов, условий, а в целом – алгоритма определения количественных значений критерия размерности для малых, средних и больших множеств альтернатив в парных сравнениях.

Предлагается в методах упорядочения альтернатив при проведении парных сравнений альтернатив принять за основу следующие принципы:

количественные значения критерия размерности малых, средних и больших множеств альтернатив в парных сравнениях взаимоувязаны с количеством альтернатив в полном блоке (r^b) и рассчитываются через r^b;

количественные значения психологического ограничения эксперта определяют выбор диапазона r^b;

в зависимости от выбираемых количественных значений r^b, критерий размерности множеств альтернатив для малых, средних и больших множеств альтернатив в парных сравнениях приобретает соответствующую динамику изменений;

количество альтернатив в полном блоке (r^b) равно количеству полных блоков в цикле парных сравнений;

за единицы шкал размерности множеств альтернатив при проведении парных сравнений могут приниматься количества альтернатив в полном блоке или количество

полных блоков в цикле парных сравнений. В этом случае A_R будет включать в себя, в зависимости от выбранной единицы размерности шкалы, следующие подмножества:

$$\begin{cases} A_r, A_R \in \{A_r \in A_R \mid r = \overline{3, r^b}\}, \\ A_z, A_R \in \{A_z \in A_R \mid z = \overline{0,(Z+1)}\}, \end{cases} \quad (13)$$

В результате проведенных исследований рекомендуется в парных сравнениях для малых, средних и больших множеств альтернатив применять шкалу с единицей размерности равной количеству альтернатив в полном блоке (r^b). А начиная с больших и сверхбольших множеств альтернатив (в циклах первого, второго, третьего порядка …) применять другую шкалу, где за единицу размерности может быть принято количество альтернатив в цикле (циклах) парных сравнений: A_ν, $A_R \in \{A_\nu \in A_R \mid \nu = \overline{0,(V+1)}\}$. В этом случае разница между количеством сравниваемых и учитываемых альтернатив может быть $\Delta_R = 2r^b, 3r^b, ..., Vr^b$ для $\nu = 2, 3, ..., V$. Для сверхбольших множеств – $\Delta_R = (r^b)^2, 2(r^b)^2, 3(r^b)^2, ..., V(r^b)^2$ и соответственно $\nu^2 = V^* - V$, при $Z^{o\nu} = Z^{o\nu^*} = 0$ ($Z^{o\nu}$ и $Z^{o\nu^*}$ – остаток полных блоков ν -го цикла), $\nu^3 = V^{2^*} - V^2$ и т.д., где ν^2, ν^3 ... – сверхциклы соответствующего порядка (циклы парных сравнений второго порядка, третьего порядка…). Работа с такими большими данными (множествами альтернатив) возможна только с применением искусственного интеллекта, и как предложение – с применением обобщенного экспертно-аналитического метода, ориентированного на многокритериальную экспертную оценку сложных систем без ограничения числа используемых альтернатив (показателей, параметров).

На основе вышеперечисленных выражений и принципов можно определить условия, при которых множества альтернатив парных сравнений разбиваются на малые, средние и большие.

Количество альтернатив (множество альтернатив) можно считать малым (с малой мощностью) при условиях:

$$Z^* = Z = 0, \quad (14)$$

в этом случае $\nu = 0$, $R < r^b$, $R = R^* = r^{ob} = r^{ob^*}$;

$$Z^* = Z = 1 \text{ и } r^{ob} = 0, \quad (15)$$

в этом случае $\nu = 0$, тогда $R = R^* = r^b$, $r^{ob^*} = r^{ob} = 0$.

Условия (14) и (15) выполняются, когда количество учитываемых альтернатив меньше или равно r^b соответственно. Данное теоретическое положение отвечает логике проведения парных сравнений и обосновывает практику экспертных оценок.

Это подтверждается результатами анализа литературы [1-9], посвященной данному вопросу, в которых для малых множеств верхним количественным значением критерия размерности следует считать число семь, а нижним – четыре, соответствующие признанным критериям психологического ограничения эксперта ($4 \le r^b \le 7$). Количество альтернатив, число которых в неполном блоке сравниваемых альтернатив составляет 2-3, согласно применяемым методам расстановки приоритетов и анализа иерархий уже упорядочены.

Количество альтернатив (множество альтернатив) можно считать средним (со средней мощностью), которые включены в первый цикл парных сравнений, при условиях

$$Z^* \ge Z \text{ и } R < R^* \le R + r^b. \quad (16)$$

$$\Delta_R = R^* - R = r^b. \quad (17)$$

В примере 2 (для $r^b = 4$) этим условиям соответствуют границы цикла $a_r^{1нг} = 5$ и $a_r^{1вг} = 20$.

Тогда для больших множеств альтернатив в парных сравнениях предлагается условие

$$Z^* > Z, R^* > R + r^b \quad (18)$$

В этом случае количество сравниваемых альтернатив большого множества будет находиться в пределах

$$R^* = [R + r^b + 1, ..., R + 2r^b]. \quad (19)$$

Для $v = 2, 3, ..., V$;

$$R^* > (R + 2r^b; R + 3r^b, ..., R + Vr^b). \quad (20)$$

Предложенные условия (14)-(19) размерности множеств альтернатив отвечают вышеприведенным принципам и теоретически обосновывают требования, предъявляемые практике проведения парных сравнений.

На основе данного обоснования целесообразно формализовать принадлежность множеств альтернатив A_R в качестве элементов (подмножеств) множества Ξ, где $\Xi \in \{A_R \in \Xi \mid r = \overline{1, R}\}$.

При этом для множества Ξ его подмножества предлагается классифицировать следующими образом: $\Xi \in \{A^{\text{М}}, A^{\text{С}}, A^{\text{Б}}\}$, где $A^{\text{М}}$ – есть подмножество малых множеств альтернатив, $A^{\text{С}}$ – подмножество средних множеств альтернатив, $A^{\text{Б}}$ – подмножество больших множеств альтернатив. Это дает возможность формализовать следующее:

$$\begin{cases} A_R \in A^{\text{М}}, \text{ если } 3 < R \le r^b, \\ A_R \in A^{\text{С}}, \text{ если } R \ge ((R^* - r^b) > 0), \\ A_R \in A^{\text{Б}}, \text{ если } R < (R^* - r^b), \end{cases} \quad (21)$$

где $3 < r^b \le 7$, а $R^* = R + Z$ при $r^{ob} > 0$ и $R^* = R + (Z - 1)$ при $r^{ob} = 0$.

Исходя из выражения (21) критерий размерности (R^{Ξ}) в парных сравнениях предоставляет собой систему количественных значений критериев размерности

$$R^{\Xi} = <R^{\text{М}}, R^{\text{С}}, R^{\text{Б}}>, \quad (22)$$

где $R^{\text{М}}$ – критерий для малых подмножеств – $A^{\text{М}}$;

$R^{\text{С}}$ – критерий для средних подмножеств – $A^{\text{С}}$;

$R^{\text{Б}}$ – критерий для больших подмножеств $A^{\text{Б}}$, при этом:

$$\begin{cases} A_R \in A^{\text{М}}, \text{ если } 3 < R^{\text{М}} \le r^b, \\ A_R \in A^{\text{С}}, \text{ если } r^b < R^{\text{С}} \le r^b(r^b + 1), \\ A_R \in A^{\text{Б}}, \text{ если } R^{\text{Б}} > r^b(r^b + 1), \end{cases} \quad (23)$$

где $3 < r^b \le 7$.

Практическим результатом применения выражений (21)-(23) являются рассчитанные и приведенные в табл. 1 элементы малых ($A^{\text{М}}$), средних ($A^{\text{С}}$) и больших ($A^{\text{Б}}$) подмножеств альтернатив для $r^b = \overline{4, 7}$.

Таблица 1 – Элементы малых, средних и больших подмножеств множества A_R

№ п/п	Количественное значение r^b	Элементы множества A_R		
		Элементы подмножества $A^{\text{М}}$	Элементы подмножества $A^{\text{С}}$	Элементы подмножества $A^{\text{Б}}$
1	7	{4, 5 , 6, 7}	{8, 9,..., 55, 56}	{57, 58,..., $R^{\text{Б}}$}
2	6	{4, 5 , 6}	{7, 8,..., 41, 42}	{43, 44,..., $R^{\text{Б}}$}
3	5	{4, 5 }	{6, 7,..., 29, 30}	{31, 32,..., $R^{\text{Б}}$}
4	4	{4}	{5, 6,..., 19, 20}	{21, 22,..., $R^{\text{Б}}$}

Заключение

В результате работы формализованы исходные данные метода парных сравнений и приведены их определения. Формализованы особенности метода парных сравнений, выраженные в функциональной зависимости количества учитываемых альтернатив в экспертных оценках и количества сравниваемых альтернатив, которые упорядочивают, из состава учитываемых альтернатив, в блоки (матрицы) парных сравнений. Разработаны принципы упорядочения альтернатив и выражения расчетов значений критерия размерности, проработанного в качестве системы критериев размерности для малых, средних и больших множеств альтернатив. Выявлена вторая особенность парных сравнений, связанная с введенными понятиями цикла парных сравнений и нижней и верхней границами цикла парных сравнений. Первая и вторая особенности парных сравнений иллюстрированы

примерами. Представлены расчеты количественных значений критериев размерности для малых, средних и больших множеств альтернатив, а также верхних и нижних границ циклов парных сравнений, исходя из выбираемого значения, от четырех до семи альтернатив, критерия психологического ограничения эксперта.

В целом разработан математический аппарат, позволяющий определять количественные значения критерия размерности множеств альтернатив в экспертных оценках, проводимых методом парных сравнений.

Частными результатами настоящей работы являются:

приведенные определения учитываемых и сравниваемых альтернатив, множеств и остатков альтернатив, полных и неполных блоков парных сравнений;

исследование второй особенности парных сравнений, а также приведенные определения цикла парных сравнений, нижней и верхней границ цикла парных сравнений;

формализованные способы расчета Z, Z^*, R, R^*, v, Δ^v_R , Z_v , Z^*_v , $R^{ивг}{}_v$, $R^{*ивг}{}_v$, $R^{инг}{}_v$, $R^{*инг}{}_v$;

формализация первой и второй особенности парных сравнений, характеризующихся соответственно полными блоками и циклами парных сравнений;

предложены единицы измерения множеств альтернатив в парных сравнениях, а именно: для малых и средних множеств это r^b – количество альтернатив в полном блоке, а для больших – количество полных блоков в цикле парных сравнений.

Практическим результатом исследований являются рассчитанные и приведенные в табл. 1 элементы малых, средних и больших множеств альтернатив для $r^b = \overline{4,7}$.

Применимость полученных результатов заключается в том, что разработанный математический аппарат дает возможность не только теоретически обосновывать выбор и рассчитывать количественные значения критериев размерности множеств альтернатив для различных аспектов экспертных оценок, но и проводить экспертные оценки со множествами, которые по своей мощности могут намного превышать множества альтернатив, рассмотренных в данной работе.

Литература

1. Дэвид Г. Метод парных сравнений. Пер. с англ. Н. Космарской и Д. Шмерлинга. Под ред. Ю. Адлера. М.: Статистика, 1978. 144 с.

2. Блюмберг В.А., Глущенко В.Ф. Какое решение лучше?: Метод растановки приоритетов. Л.: Лениздат. 1982. 160 с.

3. Саати Т., Кернс К. Аналитическое планирование. Организация систем: Пер. с англ. М.: Радио и связь, 1991. 224 с.

4. Азгальдов Г.Г., Райхман Э.П.. О квалиметрии. Издательство стандартов, 1972. 172 с.

5. Денисов А.А., Колесников Д.Н. Теория больших систем управления. Учебное пособие для вузов. – Л.: Энергоиздат, 1982. 288 с.

6. Бешелев С.Д., Гурвич Ф.Г. Экспертные оценки. М.: Наука, 1973. 161 с.

7. Методические указания. Комплексная оценка технического уровня продукции. РД 45.091.000-90

8. Методические указания по оценке технического уровня систем и аппаратуры связи, передачи и обработки информации. М.: МО СССР, 1985. 45 с.

9. Бояринцев А.В. Основы оценки эффективности систем связи ВМФ. – СПб.: Региональная общественная организация научных работников «Центр Поддержки Научных Исследований», 2001. 54 с.

References

1. David G. *Metod parnyh sravnenij* [Method of paired comparisons]. Lane from English N. Kosmarskaya and D. Schmerling. Ed. Yu. Adler. With the attached to the Russian translation. Moscow, Statistics, 1978. 144 p. (in Russian).

2. Blumberg V.A., Glushchenko V.F. *Kakoe reshenie luchshe?* [What better solution?]. Method of prioritization. Lwningrad. Lenizdat, 1982. 160 p. (in Russian).

3. Saati T., Kearns K. *Analiticheskoe planirovanie. Organizaciya sistem* [Analytical planning. Organization of systems]. Per. from English. Moscow. Radio and communications, 1991. 224 p. (in Russian).

4. G.G. Azgaldov, E.P. Reichman. *O kvalimetrii* [About qualification]. Standards Publishing House, 1972, 172 p. (in Russian).

5. Denisov A.A., Kolesnikov D.N. *Teoriya bol'shih sistem upravleniya* [Theory of large control systems]. Textbook for universities. Leningrad. Energoizdat, 1982. 288 p. (in Russian).

6. Beshelev S.D., Gurvich F.G. *Ekspertnye ocenki* [Expert assessments]. Moscow. Science, 1973. 161 p. (in Russian).

7. Methodological guidelines. *Kompleksnaya ocenka tekhnicheskogo urovnya produkcii* [Comprehensive assessment of the technical level of products]. RD 45.091.000-90 (in Russian).

8. *Metodicheskie ukazaniya po ocenke tekhnicheskogo urovnya sistem i apparatury svyazi, peredachi i obrabotki informacii* [Methodological guidelines for assessing the technical level of communication systems and equipment, transmission and processing of information]. Moscow. MO SSSR. 1985. 45 p. (in Russian).

9. Boyarintsev A.V. *Osnovy ocenki effektivnosti sistem svyazi VMF* [Fundamentals of assessing the effectiveness of communication systems of the Navy]. St. Petersburg: Regional public organization of scientists «Center for Support of Scientific Research», 2001. 54 p. (in Russian).

Статья поступила 18 сентября 2020 г.

Информация об авторах

Севастьянов Степан Иванович – Кандидат технических наук. Начальник сектора ПАО «Интелтех». Адрес: 197342, Россия, г. Санкт Петербург, ул. Кантемировская, д. 8. Тел. 8-911-702-44-52.

Criterion of dimensionality of sets of alternatives in expert assessments carried out by the method of paired comparisons

S.I. Sevastyanov

Annotation. *The article addresses* ***the problem*** *of choosing and formalizing the criterion of the dimension of sets of alternatives in expert assessments conducted by the method of paired comparisons.* ***The purpose of the work*** *is to develop a mathematical apparatus that allows you to determine the quantitative values of the dimension criterion of sets of alternatives.* ***Novelty:*** *a system of dimensionality criteria has been developed for small, medium and large sets of alternatives. A second feature of paired comparisons was revealed, associated with the introduced concepts of a "cycle of paired comparisons" and "lower and upper boundaries of a cycle of paired comparisons."* ***The result:*** *the initial data of the method of paired comparisons are formalized, their definitions are given. Peculiarities of pair comparison method expressed in functional dependence of number of considered alternatives in expert estimates and number of compared alternatives, which are ordered, from composition of considered alternatives, into blocks (matrices) of pair comparisons, are formalized. The principles of ordering alternatives and expressing calculations of the values of the dimensionality criterion developed as a system of dimensionality criteria for small, medium and large sets of alternatives have been developed. The first and second features of paired comparisons are illustrated by examples. There are presented calculations of quantitative values of dimensionality criteria for small, medium and large sets of alternatives, as well as upper and lower boundaries of cycles of paired comparisons, based on the selected value, from four to seven alternatives, the expert's psychological restriction criterion.* ***Conclusions****: a mathematical apparatus has been developed that allows you to determine the quantitative values of the criterion for the dimensionality of sets of alternatives in expert estimates conducted by the method of paired comparisons.* ***The practical significance*** *is that the developed mathematical apparatus makes it possible not only to theoretically justify the choice and calculate quantitative values of the criteria for the dimensionality of sets of alternatives for various aspects of expert assessments, but also to conduct expert assessments with sets that can far exceed the many alternatives considered in the article.*

Keywords: *expert assessment, expert psychological restriction criterion; methods and features of paired comparisons; small, medium and large alternatives; dimension criterion; a cycle of paired comparisons; lower and upper boundaries of the pairwise comparison cycle.*

Information about Authors

Sevastyanov Stepan Ivanovich – Doctoral. Head of Sector of the Inteltech. Tel.: +7-911-702-44-52. Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya st., 8.

Для цитирования: Севастьянов С.И. Критерий размерности множеств альтернатив в экспертных оценках, проводимых методом парных сравнений // Техника средств связи. 2020. № 3 (151). С. 80-90.

For citation: Sevastyanov S.I. Criterion of dimensionality of sets of alternatives in expert assessments carried out by the method of paired comparisons. Means of communication equipment. 2020. No 3 (151). Pp. 80-90 (in Russian).

УДК 623.832

Унификация базовых несущих конструкций II и III уровней в комплексах связи для военно-морского флота

Михайлюк П.П., Малаева Е.А.

Аннотация. Постановка задачи*: унификация конструктива при производстве основных несущих конструкций для обеспечения гибкости при проектировании и изготовлении.* ***Целью работы*** *является анализ и описание текущего состояния унификации при изготовлении основных несущих конструкций.* ***Новизна****: состоит в рассмотрении вопроса сохранения тактико-технических характеристик прибора на примере электро-магнитной совместимости при унификации конструкции.* ***Результат****: заключается в том, чтобы проиллюстрировать принципы унификации при изготовлении терминалов малой серийности с небольшими отличиями в базовых несущих конструкциях.* ***Практическая значимость****: проанализированы конкретные примеры унификации использования съемной панели разъемов при изготовлении корпуса прибора, стоек и самих устройств.*

Ключевые слова*: унификация; стандартизация; каталогизация; базовая несущая конструкция.*

Введение

Проблема унификации базовых несущих конструкций (БНК) актуальна, поскольку на основе принципов стандартизации, унификации и нормативных актов взаимозаменяемости формируются методологии технических измерений, а также системы менеджмента качества и сертификации продукции.

Стандартизация напрямую влияет на повышение эффективности производства, являясь научным методом оптимального упорядочения номенклатуры и качества продукции внутри государства. Стандарт и качество неразделимы.

При разработке продукции радиоэлектронной аппаратуры (РЭА) уровень внутрипроектной и межпроектной стандартизации и унификации рассчитывается в соответствии с ГОСТ РВ 20.39.309-98, ГОСТ РВ 15.207-2005 [1, 2]. В этом случае коэффициенты применимости составных частей изделий не должны быть меньше требований, указанных в техническом задании (ТЗ). Обычно эти значения являются следующими:

– на уровне детализации – 50%;

– на уровне сборочных единиц – 30%.

Коэффициенты повторения составных частей изделий должны быть не менее:

– на уровне детализации – 4;

– на уровне сборочной единицы – 1.

Показатели стандартизации и унификации описывают насыщение продукции стандартными, унифицированными и оригинальными компонентами, а также уровень унификации с другими продуктами, то есть степень использования в конкретном изделии стандартизированных деталей, сборочных единиц, блоков и других составных частей изделия.

Данные показатели определяют степень однородности конструкции изделия. Они показывают возможность использования минимально необходимого количества типономиналов составных частей изделия для повышения качества продукта и эффективности производства [3].

Обоснование количественных требований к стандартизации и унификации разработанного изделия осуществляется на основе анализа статистических данных по

показателям стандартизации и унификации ранее разработанной продукции и взаимосвязи с технико-экономическими и эксплуатационными характеристиками.

Основными целями объединения являются:

– сокращение множества доступных видов, типов и типоразмеров вооружения и военной техники (ВВТ) той же функциональной цели путем изменения, при необходимости, конструкций или конструктивных элементов, основных и второстепенных размеров, и т. д.;

– изменения в конструкции и исполнительных размерах, марок материалов, технической и термохимической обработки, точного изготовления аналогичных деталей, используемых на различных заводах, в целях внедрения автоматических линий, обеспечивающих экономичную перерегулировку с заданными размерами серийного производства деталей;

– создание комплексов взаимозаменяемых агрегатов, узлов и деталей, предназначенных для сборки гораздо большего ассортимента вооружения и военной техники путем добавления определенного количества специальных узлов и деталей;

– пересмотр видов, типов и типоразмеров выпускаемых или приобретаемых для ВВТ-пакета с целью замены устаревших или недостаточно качественных на более современные, надежные и долговечные изделия.

Проведение унификации, сопровождаемое определенными затратами, требует экономического обоснования. Необоснованная унификация может иметь отрицательный эффект, особенно когда необходимо использовать ближайшие крупные унифицированные детали, вызывая неоправданные рабочие условия, увеличение веса, габариты и трудоемкость производственных машин.

На рис. 1 показана зависимость экономического эффекта от типа производства. Кривая 1 описывает изменение экономического эффекта в зависимости от уменьшения типичных размеров продукции и, как следствие, увеличения объёма выпуска, то есть специализации производства. Кривая 2 описывает затраты, связанные с унификацией.

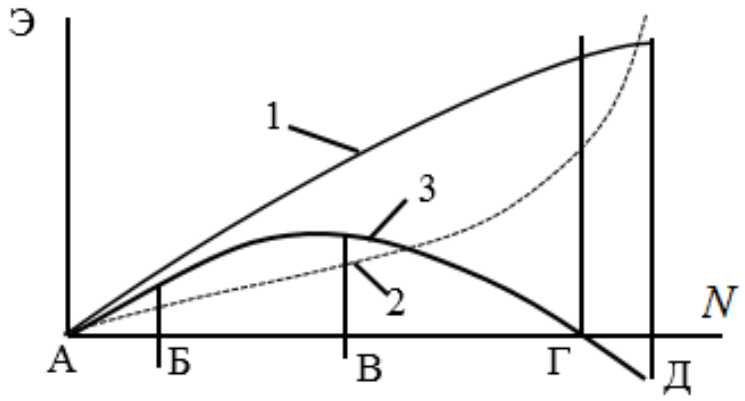


Рис.1. Зависимость экономического эффекта от вида производства

Кривая 3 описывает общий экономический эффект, достигнутый за счет улучшения качества продукта и эффективности производства. На участке АБ эффективность и затраты, связанные с унификацией, очень низкие. На участке БВ общая эффективность резко возрастает и достигает пика в точке В. Дальнейшее сокращение типов и увеличение серийной эффективности малоэффективны в производственной сфере, так как специализация уже реализована, расходы продолжают расти (участок ВГ). На участке ГД дальнейшее уменьшение размера экономически неэффективно [4, 5].

1 Сущность блочно-модульного метода проектирования

Снизить затраты на разработку, подготовку производства и освоение РЭА, обеспечить совместимость и преемственность аппаратурных решений с одновременным улучшением качества, увеличением надежности и срока службы аппаратуры в эксплуатации позволяет модульный принцип конструирования изделий. Модульный принцип конструирования предусматривает проектирование изделий РЭА на основе максимальной конструктивной и функциональной взаимозаменяемости составных частей конструкции – модулей.

В основе модульного принципа лежит разукрупнение (разбивка, расчленение) электронной схемы РЭА на функционально законченные подсхемы (части), выполняющие определенные функции. Эти подсхемы разбиваются на более простые модули, и так далее, пока электронная схема изделия не будет представлена в виде набора модулей различной сложности, а низшим модулем не окажется корпус микросхемы (МС) с обслуживающими ее радиоэлементами.

В зависимости от сложности проектируемого изделия может быть задействовано разное количество уровней модульности. Конструкция современной РЭА является иерархией модулей, каждая ступень которой называется уровнем модульности.

В конструкции радиоэлектронной аппаратуры можно выделить четыре основных уровня.

Уровень 0 Конструктивно неделимый элемент – интегральная микросхема с радиоэлементами ее обслуживания.

Слой I. На уровне I неделимые элементы объединены в схемные комбинации, имеющие более сложную функциональную особенность, образующие ячейки, модули. Первый структурный уровень, например, включает в себя печатные платы и большие гибридные интегральные схемы.

Уровень II. Этот уровень включает в себя конструктивные единицы – блоки, предназначенные для механического и электрического объединения элементов уровня I. Основными конструктивными элементами блока являются панели с соответствующими разъемами модулей первого уровня. Межмодульная коммутация выполняется соединителями, расположенными по периферии панели блока. Модули первой уровня размещаются в один или несколько рядов.

Уровень III может быть реализован в виде каркаса, стойки или большого прибора, внутренний объем которых заполняется конструктивными единицами уровня II – блоками.

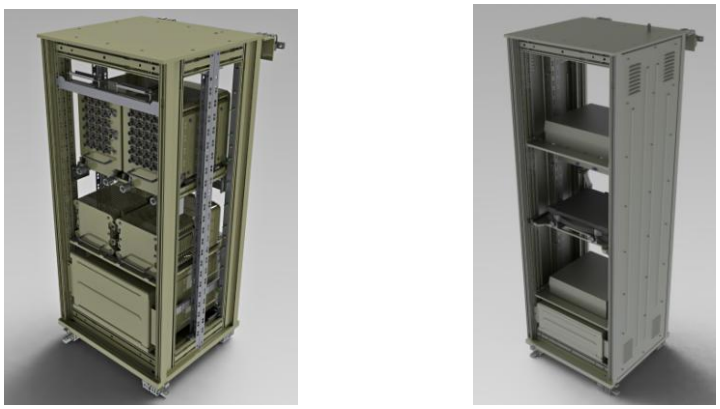
Выбор способа изготовления печатных плат и технологического оборудования для их изготовления накладывает ограничения на стандартные размеры печатных плат, что в конечном счете создает очень сложную задачу для разработчика. Поэтому для упрощения данной задачи разработана и широко используется нормативно-техническая документация, регулирующая типоразмеры печатных плат. Ее использование способствует унификации типов печатных плат и конструкций ячеек.

2 Технические решения стойки телекоммуникационной

Работа в области унификации выборки ВВТ характеризуется уровнем унификации – насыщением выборки ВВТ унифицированными и стандартными компонентами. В этом случае уровень должен быть оптимальным. Все компоненты образца не могут быть стандартными или унифицированными. Полная стандартизация ограничит идею инноваций. Если в образце не используются стандартные и унифицированные изделия, конструктору придется разрабатывать существующие и технологически отлаженные детали или сборки. Соотношение унифицированной и оригинальной продукции должно быть оптимальным, тогда достигается максимально возможная технико-экономическая эффективность для обеспечения заданных технических характеристик образца.

Очень часто при разработке оборудования с использованием блочно-модульного метода проектирования основными несущими конструкциями транспортного средства являются корпуса и каркасы, разработанные на основе так называемой «Евромеханики».

Например, возьмем универсальную БНК стойки ЗАС1, представленную на рис. 2а, и стойки КПС, рис. 2б, позволяющую изменять ее внутреннее наполнение в зависимости от выполняемых задач. Одна и та же конструкция стойки может применяться в разных изделиях.



а) б)

Рис. 2. Стойка ЗАС1 (а), стойка КПС (б)

В настоящее время широко используются 19-дюймовые конструкции согласно МЭК 297 (формат 482,6 мм). Основной единицей измерения в МЭК 297 является дюйм, который считается равным 25,4 мм. Это позволяет достаточно удобно пользоваться им в странах с метрической системой измерения. Ширина кассет и субблоков для установки в стойку составляет 482,6 мм. Однако под посадочные места для модулей зарезервирована не вся ширина субблоков, а только 16,8 дюймов или 426,72 мм. Это пространство делится на 84 посадочных места шириной 5,08 мм или 0,2 дюйма. Все вертикальные посадочные размеры в шкафах кратны 44,45 мм, что составляет 1,75 дюйма.

Важным этапом проектирования модулей первого уровня является выбор их типоразмеров. Известно, что это в первую очередь определяется тактическими и техническими требованиями на аппаратуру, которые задают основные условия эксплуатации и габариты изделия.

3 Технические решения приборов «Модуль доступа» и «Коммутатор доступа»

Рассмотрим универсальную БНК модуля доступа (МД), показанную на рис. 3, позволяющую адаптировать устройство к различным методам установки.

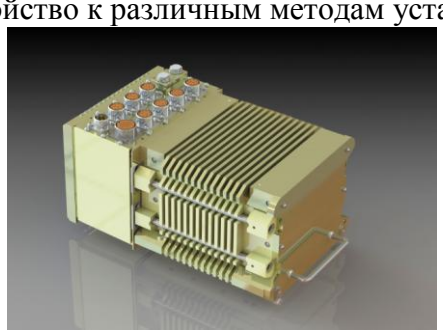


Рис. 3. Модуль доступа

Каркас для МД унифицирована с задней платой ввода-вывода (ПВВ), а съемный блок содержит деталь, уникальную для каждой версии устройства, которая позволяет не влиять на большую часть конструкции при внесении изменений (рис. 4).

Рис. 4. Унифицированная часть с ПВВ

Унификация в БНК коммутатора доступа также позволяет размещать различное содержимое в устройстве без изменения центральной части устройства, без изменения местоположения и точек крепления, меняя только переднюю и заднюю крышки. Это хорошо видно на шлюзе сопряжения, удаленном устройстве питания, коммутаторе доступа и сервер-коммутаторе рис. 5.

Рис. 5. Унификация в БНК коммутатора

Применяя принцип блочно-модульного метода проектирования РЭС, можно создать систему с практически неограниченной производительностью и сложностью, сохраняя при этом гибкость в ее организации, поскольку разработчик использует ровно столько модулей, сколько ему требуется. Разработчик системы также может легко модернизировать конструкцию, изменив или добавив отдельные модули и получив необходимые параметры.

4 Технические решения терминала многофункционального

Проанализируем техническое решение на примере универсальной БНК корпуса терминала многофункционального (ТМ), показанной на рис. 6, позволяющей настраивать и заменять электронные узлы и адаптировать устройство к различным методы установки и крепления.

Рис. 6. Универсальная конструкция

Одним из технических решений, иллюстрирующих принцип стандартизации и унификации является съемная панель (рис. 7).

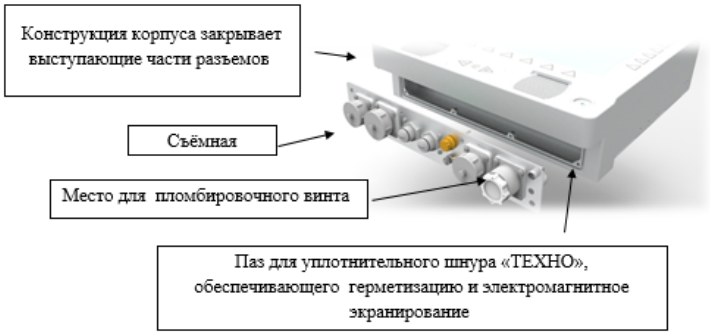


Рис. 7. Съемная панель

Съемная панель разъемов представляет собой комплектный съемный блок с электромонтажом. При необходимости это решение позволяет изменить внутреннее наполнение устройства без повторного изготовления корпуса (за исключением съемной панели). Съемная панель позволяет предоставить возможность замены или изменения количества разъемов на панели.

Одним из технических решений является съемная виброразгрузочная платформа, показанная на рис. 8.

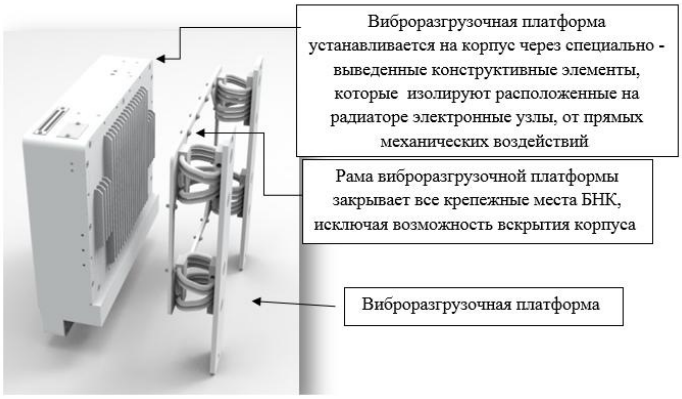


Рис. 8. Виброразгрузочная платформа

Конструкция БНК позволяет заменить виброразгрузочную платформу универсальной рамой, которая адаптирует БНК к дополнительным способам установки и крепления.

При унификации БНК часто возникает проблема сохранения электромагнитной совместимости. Дополнительные стыки между съемными частями корпуса выполняются в виде «замка» для создания лабиринта, который увеличивает потери при прохождении электромагнитной волны через зазор. «Замок» дополнительно содержит токопроводящий профиль, показанный на рис. 9.

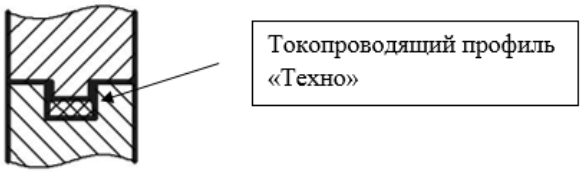


Рис. 9. Токопроводящий профиль

Также между разъемными частями корпуса проложены профили из токопроводящего силикона (рис. 10).

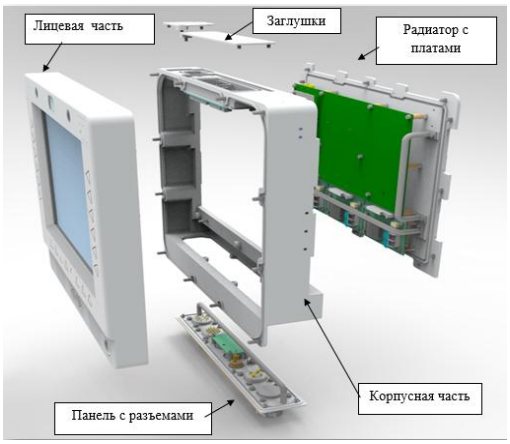


Рис. 10. Разъемные части корпуса

Подобные решения позволят достигнуть защиты от ЭМС и унифицировать БНК терминала.

Вывод

Рассмотренный в статье пример показывает, что конструктору при унификации БНК важно учитывать вопросы сохранения технических характеристик, особенно в части ЭМС, а также необходимо сочетать их с улучшением экономических характеристик производства. Параметрическая стандартизация используется для установления рациональной номенклатуры выпускаемой продукции с целью унификации, увеличения серийности и развития специализации их производства. Для этого разрабатывают стандарты для параметрических рядов этих изделий.

Литература

1. ГОСТ РВ 20.39.309-98 Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Конструктивно-технические требования. М.: Госстандарт России, 1998.

2. ГОСТ РВ 15.207-2005 Военная техника. Порядок проведения работ по стандартизации и унификации в процессе разработки и постановки на производство изделий. М.: Госстандарт России, 2005.

3. Димов Ю.В. Метрология, стандартизация и сертификация. Издательский дом «Питер». 2010. 463 с.

4. Никифоров А.Д, Бакиев Т.А. Метрология, стандартизация и сертификация. М. Высш. школа. 2002. 422 с.

5. Миньков С.Л. Технико-экономическое обоснование выполнения проекта: методическое пособие. Томск: ТУСУР, 2014. – 30 с.

References

1. GOST RV 20.39.309-98 Complex system of General technical requirements. Equipment, devices, devices and equipment for military purposes. Design and technical requirements. Moscow. Gosstandart of Russia. 1998 (in Russian).

2. GOST RV 15.207-2005 Military equipment. Procedure for standardization and unification during the development and commissioning of products. M.: Gosstandart of Russia. 2005 (in Russian).

3. Dimov Yu.V., Metrology, standardization and certification. Piter. 2010. Pp. 463 (in Russian).

4. Nikiforov A.D, Bakiev T.A. Metrology, standardization and certification. Moscow. High school. 2002. Pp. 422 (in Russian).

5. Minkov S.L., Feasibility study of the project: methodological guide. Tomsk: TUSUR, 2014. – 30 seconds (in Russian).

Статья поступила 21 сентября 2020 г.

Информация об авторах

Михайлюк Павел Петрович – Кандидат технических наук, доцент кафедры института Фундаментальной подготовки и технологических инноваций Санкт-Петербургского государственного университета аэрокосмического приборостроения. MBA Технический директор ПАО «Интелтех». Тел.: +7-911-257-16-65. E–mail: mihayluk@inteltech.ru.

Малаева Екатерина Александровна – Аспирант Томского политехнического университета по направлению Техносферная безопасность. Тел.: +7-913-110-78-37. E–mail: katrina.malaeva@bk.ru.

Адрес: 197342, Россия, г. Санкт-Петербург, Кантемировская, 8.

Unification of basic load-bearing structures of the II and III levels in communication complexes for the Navy

P.P. Mikhaylyuk, E.A. Malaeva

Annotation. ***Problem statement****: unification of constructs in the production of basic load-bearing structures to ensure flexibility in design and manufacturing. The aim of the work is the analysis and description of the current state of unification in the manufacture of basic supporting structures. Novelty: consists in examining the issue of preserving the performance characteristics of the device using the example of EMC when unifying the design. Result: it consists in illustrating the principles of unification in the manufacture of small-series terminals with slight differences in the design of the BNK. Practical relevance: specific examples of unification of the use of a removable panel of connectors in the manufacture of the device body, racks, devices themselves, are analyzed.*

Keywords*: unification; standardization; cataloging; basic supporting structure.*

Information about Authors

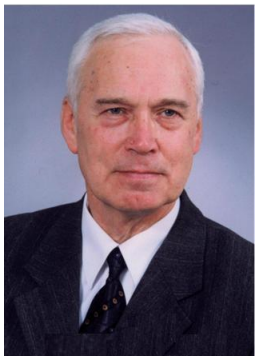
Pavel Petrovich Mihailuk - Candidate of Technical Sciences, Associate Professor of the Institute of Fundamental Training and Technological Innovation, St. Petersburg State University of Aerospace Instrumentation. MBA Technical Director, PJSC «Inteltech». Tel.: +7-911-257-16-65. E–mail: mihayluk@inteltech.ru.

Ekaterina Aleksandrovna Malaeva – Graduate student of Tomsk Polytechnic University in the field of Technosphere safety. Tel.: +7-913-110-78-37. E–mail: katrina.malaeva@bk.ru.

Address: Russia, 197342, Saint-Petersburg, Kantemirovskaya, 8.

Для цитирования: Михайлюк П.П., Малаева Е.А.Унификация базовых несущих конструкций II и III уровней в комплексах связи для ВМФ // Техника средств связи. 2020. № 3 (151). С. 91-98.

For citation: Mikhaylyuk P.P., Malaeva E.A. Unification of basic load-bearing structures of the II and III levels in communication complexes for the Navy. Means of communication equipment. 2020. No 3 (151). Pp. 91-98 (in Russian).



ПОЗДРАВЛЯЕМ!

Генеральному конструктору ПАО «Интелтех», известному ученому и конструктору в области исследований и создания средств связи для ВМФ и сухопутных войск РФ, доктору технических наук, профессору **Валентину Ивановичу Мирошникову** исполнилось 80 лет

В.И. Мирошников родился 31.10.1940 г. в Ленинграде. В 1963 г. окончил Ленинградский электротехнический институт (ЛЭТИ) им. В.И. Ульянова (Ленина) (факультет автоматики и вычислительной техники по специальности «Математические и счетно-решающие приборы и устройства»), инженер-электрик.

В 1964 г. поступил в Ленинградский НИИ-778 МПСС, в дальнейшем НИИ электротехнических устройств (НИИ ЭТУ) – головной институт ЛНПО «Красная Заря». Прошел все ступени профессионального роста, в 1980 г. стал заместителем директора по научной работе НИИ ЭТУ (с 2002 г. ОАО «Интелтех»), в 2001 г. – генеральным конструктором ОАО «Интелтех» (с 2014 г. ПАО «Интелтех»).

Один из основателей и руководителей научной школы по разработке средств глобальной связи с подводными лодками (ПЛ) и надводными кораблями (НК) по быстродействующим (БД) и сверхбыстродействующим (СБД) КВ и СДВ каналам ВМФ. Как главный и генеральный конструктор решил ряд научно-технических проблем, связанных с разработкой и производством комплексов обмена данными береговых командных пунктов (БКП) с ПЛ и НК «Дальность», «Интеграл», «Глубина», «Невка».

В 60-е гг. в качестве научного руководителя и главного конструктора внес определяющий вклад в решение задачи защиты стратегического оружия на ПЛ от несанкционированного, или случайного применения. В ОКР «Замок» обосновал возможность создания специализированного комплекса защиты, определил структуры пусковых команд и выполнил расчеты основных параметров радиолиний.

В 70-е гг. В.И. Мирошников – один из разработчиков комплекса связи «Команда», созданного по результатам ОКР «Замок». Комплекс стал основой системы дальней (более 10 000 км) оперативной связи ВМФ и обеспечивал передачу команд на применение стратегического ядерного оружия с одновременным обеспечением его гарантированной защиты от несанкционированного пуска. За работы по этой тематике В.И. Мирошникову в 1978 г. присуждена Государственная премия СССР.

В 70 - 80-е гг. В.И. Мирошников участвовал в создании командной системы управления для органов высшего государственного и военного управления. Система создавалась на принципиально новой аппаратно-программной платформе с использованием средств вычислительной техники и единых протоколов информационного обмена и информационно-технического взаимодействия радиооборудования.

На базе разработанных под руководством В.И. Мирошникова унифицированных береговых и бортовых комплексов средств автоматизации связи была создана первая в стране система обмена данными ВМФ, обеспечивающая помехозащищенный обмен формализованными сообщениями БКП с ПЛ и НК в режимах БД («берег-море») и СБД («море-берег») связи по КВ и СДВ каналам. За эту работу В.И. Мирошников в 2006 г. удостоен премии Правительства РФ в области науки и техники.

За выдающиеся научные и практические результаты по созданию нескольких поколений комплексов автоматизированной связи и обмена данными ВМФ и их внедрение в серийное производство В.И. Мирошникову в 2019 г. присуждена премия Правительства Санкт-Петербурга (премия А.С. Попова). В настоящее время В.И. Мирошников руководит работами по выполнению государственных оборонных заказов по созданию системы связи ВМФ повышенной устойчивости и надежности.

В.И. Мирошников – автор более 130 научных трудов, включая 8 монографий, более 100 статей и патентов на изобретения, внесших большой вклад в решение научно-технических проблем управления ракетно-ядерным флотом России, в теорию и практику создания средств связи для Военно-морского флота и Сухопутных войск Вооруженных Сил Российской Федерации.

В.И. Мирошников – лауреат Государственной премии СССР (1978). Почетный радист (1979), Заслуженный деятель науки РФ (1997). Лауреат премии правительства РФ в области науки и техники (2006) и премии Правительства Санкт-Петербурга (2019). Член бюро Научного совета РАН по проблеме «Радиофизические методы исследования морей и океанов», профессор базовой кафедры «Информационные системы» Санкт-Петербургского ГЭТУ. Награжден орденами «Знак Почета», «За заслуги перед Отечеством IV степени» и пятью медалями.

Руководство, коллектив ПАО «Интелтех» и редакционная коллегия журнала «Техника средств связи» поздравляют Вас, уважаемый Валентин Иванович, с юбилеем! Желаем Вам крепкого здоровья, плодотворного труда и семейного благополучия!