"Ассоциация ГЛОНАСС/ГНСС-форум"
Ваш гид в мире навигации!

Ассоциация разработчиков, производителей и потребителей оборудования и приложений на основе глобальных навигационных спутниковых систем

Ассоциация, опираясь на опыт ведущих специалистов в области использования спутниковых навигационных технологий, предлагает сотрудничество по следующим направлениям:

- консалтинг по внедрению навигационных технологий и их использованию;
- сертификация аппаратуры спутниковой навигации ГЛОНАСС/GPS и систем на ее основе;
- консультационное сопровождение при подготовке конкурсной документации по внедрению информационно-навигационных систем;
- экспертная оценка конкурсной документации и поданных заявок;
- содействие в организации международного сотрудничества;
- выполнение научно-исследовательских и опытно-конструкторских работ;
- разработка информационно-аналитических материалов;
- проведение маркетинговых исследований;
- организация и проведение мероприятий;
- нормативно-правовое обеспечение и юридическая поддержка деятельности.

Адрес: 125167, Москва, 4-ая ул. Восьмого Марта, д.3.
Тел. +7 (499) 152 31 70. Факс: +7 (499) 152 96 35. E-mail: info@aggf.ru. URL: www.aggf.ru

H&ES RESEARCH

ТОМ IV
№1-2012

Наукоёмкие технологии в космических исследованиях Земли

Учредитель
ООО "Издательский дом Медиа Паблишер"

Главный редактор: Легков К.Е.
HT-ESResearh@yandex.ru

Издатель: Дымкова С.С.
ds@media-publisher.ru

Hi-tech Earth Space RESEARCH

www.H-ES.ru

СОДЕРЖАНИЕ

CONTENT

Vol IV
No. 1-2012

H&ES RESEARCH

High technologies in Earth space research

Периодичность выхода – 4 номера в год
Стоимость одного экземпляра 500 руб.
Тираж 1000 экз. + Интернет-версия

Тематические направления:
• Вопросы развития АСУ • Физико-математическое обеспечение разработки новых технологий и средств инфокоммуникаций • Условия формирования основных стандартов подвижной связи • Проектирование, строительство и интерактивные услуги в СПС • Биллинговые и информационные технологии • Электромагнитная совместимость • Антенно-фидерное оборудование • Источники электропитания • Волоконно-оптическое оборудование и технологии • Вопросы исследования космоса • Спутниковое телевидение, системы спутниковой навигации, GLONASS, построение навигационных систем GPS • Вопросы развития геодезии и картографии • Программное обеспечение и элементная база для сетей связи • Компьютерная и IP-телефоният • Информационная и кибербезопасность • Вопросы исследования Арктики • Метрологическое обеспечение • Правовое регулирование инфокоммуникаций, законодательство в области связи • Экономика связи

Редакция

Издатель: Светлана Дымкова
ds@media-publisher.ru

Главный редактор: Константин Легков
HT-ESResearh@yandex.ru

Выпускающий редактор:
Ольга Дорошкевич
ovd@media-publisher.ru

Предпечатная подготовка
ООО "ИД Медиа Паблишер"
www.media-publisher.ru

Адрес редакции
111024, Россия, **Москва**,
ул. Авиамоторная, д. 8, офис 512-514
Тел.: +7 (495) 957-77-43

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

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.

Hi-tech Earth Space RESEARCH **www.H-ES.ru**

Исследование динамических свойств коммуникационных протоколов цифровых сетей связи

Известно, что доказательство динамических свойств протоколов, обеспечивающих достаточные условия корректности его функционирования требует учета внутренних операций с данными. Для доказательства наличия свойства у проектируемого протокола необходимо исследование его пространственно-временную модель на предмет отсутствия временных блокировок, таким образом модель протокола должна обладать следующим свойством: любое состояние модели, при котором происходит динамическая блокировка через определенное спецификацией время должно меняться на принципиально новое состояние. Рассмотрен вопрос исследования динамических свойств коммуникационных протоколов цифровых сетей связи.

Ключевые слова: *динамические свойства, протокол, сеть связи, свойства, модель.*

Донченко А.А., Кисляков М.А.,
Ростовский военный институт ракетных войск им. главного маршала артиллерии М.И.Неделина

Research of dynamic properties communication protocols of digital networks communication

Donchenko A.A., Kislyakov M.A.,
The Rostov military institute of missile armies of the chief marshal of artillery M.I.Nedelin

Abstract

It is known that the proof of dynamic properties of the protocols providing sufficient conditions of a correctness of its functioning requires the accounting of dataful internal operations. The proof of existence of property at the projected protocol requires research its spatio-temporal model regarding absence of temporal locks, thus the model of the protocol shall possess the following property: any status of model in case of which there is a dynamic lock through time defined by the specification shall change on essentially new status. In article the question of research of dynamic properties of communications protocols of digital networks of communication is considered.

Keywords: *dynamic properties, protocol, communication network, properties, model.*

Исследование динамических свойств протоколов современных цифровых сетей связи (ЦСС) связано с анализом динамики функционирования протокола, т. е. характером множеств возможных последовательностей реализаций событий протокола во времени.

К динамическим свойствам протоколов относятся свойства [1]:

1. Отсутствие динамических блокировок. Это значит, что в протоколе отсутствует бесконечный цикл функционирования, при котором не производится полезная работа. Различают динамические блокировки, выход из которых логически невозможен (1а), и динамические блокировки, являющиеся следствием определенных временных характеристик протокола (1б), например темпа обмена сообщениями.

2. Завершаемость (развитие), т. е. протокол всегда достигает конечного (терминального) состояния. Для циклических протоколов это свойство несколько видоизменяется. Эти протоколы должны обладать свойством развития, которое состоит в том, что протокол достигает своего начального состояния.

3. Самосинхронизация (восстановление после ненормальной ситуации). Это свойство подразумевает, что после возникновения ненормальной ситуации протокол за конечное время восстановит свое корректное функционирование.

Доказательство динамических свойств протоколов, обеспечивающих достаточные условия корректности функционирования протокола [2], — требует учета внутренних операций с данными.

Для доказательства наличия свойства 1б у проектируемого протокола необходимо исследование его пространственно-временную модель (ПВМ) [3] на предмет отсутствия временных блокировок. Т. е., модель протокола должна обладать следующим свойством: любое состояние модели, при котором происходит динамическая блокировка через определенное спецификацией время должно меняться на принципиально новое состояние.

Свойство 2 (завершаемость) для динамической модели протокола интерпретируется как достижимость в сетевой модели некоторой разметки M_i, соответствующей конечному (терминальному) состоянию модели. В общем случае протокол может иметь некоторое множество конечных состояний $s_k=\{s_i\}$.

Таким образом, доказательство свойства 2 сводится к решению задачи достижимости для некоторого множества $\overline{M}$ терминальных разметок сети:

$$\exists \overline{M} = \{M_i\} M_1 \in \overline{M}, M_2 \in \overline{M}, ..., M_k \in \overline{M}, i = \overline{1,k}$$

где k — число конечных состояний протокола.

Свойство 3 (самосинхронизация) определяется, также как и свойство 1б, временными характеристиками протокола. Наличие данного свойства у протокола достигается за счет коррекции спецификации протокола в ходе исследования ПВМ протокола.

Как отмечалось [3], наличие у протокола свойств 1б — 3 означает его живость, т. е. протокол, обладающий указанными свойствами, в любом случае достигнет желаемого состояния.

Таким образом, для доказательства наличия динамических свойств у исследуемого протокола необходимо доказать, что он является живым.

Утверждение: Протокол является живым тогда, и только тогда, когда все множество последовательностей срабатывания переходов его пространственно-временной модели ведет к некоторой конечной разметке M_k, являющейся отображением конечного состояния протокола.

Доказательство. Пусть $EN \rightarrow PR$, $M_k \rightarrow s_k$, где s_k – конечное состояние протокола, T^* множество всех последовательностей срабатывания переходов сети EN, $L(EN, M_k) \in T^*$ – подмножество последовательностей срабатывания переходов сети EN, ведущих к M_k.

Предположим, что $T^* \neq L(EN, M_k)$. Тогда разницу множеств T^* и $L(EN, M_k)$ можно записать как:

$T^* \setminus L(EN, M_k) = T^{**} \neq \varnothing$.

То есть для сети EN существует хотя бы одна последовательность срабатываний переходов $\tau \in T^{**}$ не приводящая к M_k. Следовательно, протокол PP не является живым, или протокол PR может быть живым только тогда, когда все множество последовательностей срабатывания переходов его динамической модели ведет к некоторой конечной разметке M_k:

$T^* = L(EN, M_k)$.

Если $T^* \neq L(EN, M_k)$, то разницу множеств T^* и $L(EN, M_k)$ можно записать как:

$T^* \setminus L(EN, M_k) = \varnothing$.

То есть все последовательности срабатываний переходов $\tau \in T^*$ сети EN приводят к M_k. Так как $EN \rightarrow PR$ и $M_k \rightarrow s_k$, то протокол PR всегда достигает своего конечного состояния s_k, то есть протокол PR живой.

Иначе, если все множество последовательностей срабатывания переходов его динамической модели ведет к некоторой конечной разметке M_k, являющейся отображением конечного состояния протокола s_k, то протокол является живым.

Утверждение доказано.

Исходя из вышесказанного, анализ протокола на наличие у него динамических свойств можно осуществлять методом функционального тестирования его ПВМ, разработанной на основе аппарата EN.

Функционирование переходов такой модели на содержательном уровне можно описать следующим образом.

При поступлении метки во входную позицию p_i перехода t (рис. 1) инициируется процедура проверки готовности перехода к срабатыванию (проверяется необходимое условие его срабатывания – C).

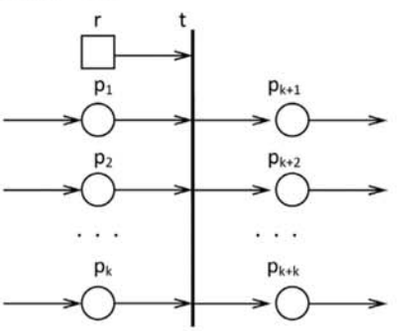


Рис. 1. Анализируемый переход

В случае истинности условия C, т.е. при соответствующей разметке входных $M(^\bullet P(t))$ и выходных позиций перехода $M(P^\bullet(t))$, производится переход к анализу состояния разрешающей позиции $m_j(r)$. Если условия разрешения и запуска перехода не выполнены, обработка перехода прекращается и запускается процедура проверки следующего перехода сети. Анализ разметки разрешающей позиции преследует цель проверить утверждение:

$m_j(r) \in M(r)$,

где $M(r)$ – множество допустимых разметок позиции r. В случае выполнения данного условия, на текущем этапе осуществляется вычисление функции преобразования атрибутов меток $\rho(t)$ и значения функции временной задержки $\tau(t)$. При достижении всех заданных условий переход вступает в активную фазу, содержание которой определяется процедурой $\Psi(t)$ и функцией $\tau(t)$ данного перехода. С началом активной фазы запускается счетчик модельного времени, обрабатывающий в заданных единицах время выполнения события.

Процедура $\Psi(t)$ выполняется в два этапа. Сначала находятся истинные предикаты выражений:

$$r_1 = \{\Pi_1 \rightarrow X_1, \Pi_2 \rightarrow X_2, ..., \Pi_n \rightarrow X_n\},$$
$$r_2 = \{H_1 \rightarrow Y_1, H_2 \rightarrow Y_2, ..., H_m \rightarrow Y_m\},$$

а затем реализуется требуемое подмножество операций над атрибутами меток $\{f_i(a_k(p_i))\}$. Далее переход вступает в завершающую фазу, на которой осуществляется смена разметки сети

$$\forall p \in P, m'(p) = m(p) - I(p,t) + Q(t,p) \quad (1)$$

и запись новых значений переменных величин атрибутов в память. Завершается функционирование перехода фиксированием состояния модельных часов и суммированием $\Delta\tau = \tau_i'' - \tau_i^к$ с накопленным ранее модельным временем. В ситуации, когда выполнены условия для запуска сразу нескольких переходов счетчик модельного времени запускается после подготовки всех переходов к срабатыванию и фиксирует наименьшее время срабатывания из $\tau(t_j)$:

$$\min \Delta\tau = \tau_i'' - \tau_{ij}^к, \quad (2)$$

где t_j – переход с наименьшим временем срабатывания из запущенных в данный момент.

После срабатывания t_j модельное время останавливается, запоминается остаток времени на активную фазу прерванных переходов и осуществляется проверка готовности к запуску неактивных на данный момент переходов. После окончания процедуры проверки восстанавливается отсчет модельного времени, продолжается активная фаза у прерванных переходов и начинается у вновь запущенных.

Функциональное тестирование заключается в решении на ПВМ протокола задачи достижимости некоторой терминальной разметки M_{TS} (соответствующей желаемому конечному состоянию протокола) с учетом параметров времени и атрибутов пришедшей в требуемую позицию метки.

В соответствии с вышеперечисленным алгоритм функционального тестирования ($A_ф$) протокола может быть записан в следующем виде.

Алгоритм A_Φ

Исходные данные: Пространственно-временная модель протокола в виде помеченной $EN = \langle P, T, I, Q, M, G \rangle$, с начальным состоянием памяти G_0 и маркировкой M_0.

Начальная установка: формируемое базовое множество достижимых маркировок $M = 0$; текущая маркировка $M_l = M_0$; текущее множество непроанализированных переходов возбужденных при M_l, $\bar{T}(M_l) = T(M_l)$; ключевая последовательность $\sigma_k = < >$; начальное модельное время $\tau_k = 0$; терминальное состояние, проверяемое на достижимость M_{TS}.

Шаг 1

1.1. Если M_l – нециклическая маркировка, и $M_l \neq M_{TS}$, то к множеству M присоединяется M_l, переход на шаг 2.

1.2. Если $M_l = M_{TS}$, переход на шаг 5.

1.3. Если M_l – циклическая маркировка, то переход на шаг 4.

Шаг 2

2.1. Для всех $t_j \in T(EN)$ проверяются условия c, r_1 и r_2. Переходы, для которых справедливы эти условия, включаются в $\bar{T}(M_l)$.

2.2. Если $\bar{T}(M_l) = \varnothing$, $\sigma_k = < >$, $l = 0$, то переход на шаг 5.

2.3. Если $\bar{T}(M_l) = \varnothing$, $\sigma_k = < >$, $l \neq 0$, то переход на шаг 4.

2.4. Если $\bar{T}(M_l) \neq \varnothing$, то переход на шаг 3.

Шаг 3

3.1. Из $\bar{T}(M_l)$ выбирается t_j с минимальным j по всем $t \in \bar{T}(M_l)$.

3.2. t_j исключается из $\bar{T}(M_l)$ и приписывается к σ_k.

3.3. l увеличивается на 1.

3.4. Формируются множества позиций, участвующих в срабатывании перехода по предикатам функций r_{1j} и r_{2j}.

3.5. Вычисляется маркировка M_{l+1}, полученная из M_l в результате срабатывания t_j: $\left(M_l \left| \frac{t_j}{} \right. M_{l+1} \right)$, полученная маркировка считается далее текущей.

3.6. Над вектором атрибутов каждой входной позиции p_k $A(p_k) = \{a_1, a_2, \ldots, a_n\}$ выполняются преобразования, заданные функцией $\rho(t_j)$.

3.7. Вычисляется новое состояние памяти G_{l+1}, полученное в результате срабатывания t_j, которое далее считается текущим.

3.8. Вычисляется значение функции временной задержки $\tau(t_j)$ и суммируется с τ_k.

3.9.Переход на шаг 1.

Шаг 4

4.1. Из σ_k исключается последний переход t_j.

4.2. l уменьшается на 1.

4.3. τ_k уменьшается на $\tau(t_j)$.

4.4. Вычисляется маркировка M_{l-1}, из которой получилась M_l в результате срабатывания $\left(M_{l-1} \left| \frac{t_j}{} \right. M_l \right)$, полученная маркировка считается текущей.

4.5. Вычисляется состояние памяти G_{l-1}, полученное состояние считается текущим.

4.6.Переход на шаг 2.

Шаг 5

Конец алгоритма.

Разработанный на основе данного алгоритма метод функционального тестирования динамической модели протоколов ЦСС, отличающийся от известных возможностью решения задачи достижимости для пространственно-временной модели протокола с учетом влияния внутренних параметров протокольных данных позволяет на базе сформированного множества достижимых терминальных разметок M_{TS} получить детерминированную оценку динамических свойств протокола и сформулировать вывод о качестве его построения по значению целевой функции F_{PR} [3] .

Литература

1. *Анисимов Н.А.* Методы формального описания, верификации и реализации сетевых протоколов с использованием теории сетей Петри. Препринт. Владивосток ИАПУ ДВНЦ АН СССР, 1984. – 40 с.

2. *Донченко А.А., Езимов А.В., Кисляков М.А.* Расширение математического аппарата Е-сетей для моделирования структурно-функциональной организации систем радиосвязи // Известия Волгоградского государственного технического университета: Межвуз. Сборн. науч. статей./ ВолГТУ. – Волгоград, 2008. – Вып. 5. – С. 140-143.

3. *Донченко А.А., Езимов А.В.* Динамическая модель протокола установления виртуального соединения пакетной сети // Теория и техника радиосвязи: Науч.-техн. сб. / ВНИИС. – Воронеж, 2002. – Вып. 1. – С. 29-35.

Мониторинг телекоммуникационных сетей в условиях чрезвычайных ситуаций

Рассмотрена система мониторинга телекоммуникционных сетей в условиях чрезвычайных ситуаций. Решена проблема обнаружения скачков интенсивности информационных потоков, свидетельствующих о неисправности сети. Приведен пример.

Ключевые слова: *мониторинг, дискретный марковский процесс с двумя состояниями, информационные потоки.*

Мелешин А.С., Хуторцева М.В.,
Северо-Кавказский филиал Московского технического университета связи и информатики

Настоящее время характеризуется опасностью возникновения чрезвычайных ситуаций (ЧС), в том числе и крупномасштабных. В этих условиях обычно нарушается система управления и жизнеобеспечения зоны ЧС. Планами управления в зоне ЧС предусматривается развёртывание мобильных радиосетей для обеспечения инфотелекоммуникационных услуг. В таких случаях наиболее удобной для развертывания и дальнейшей эксплуатации является транкинговая радиосеть. Такие сети, как правило, используются специальными службами для обеспечения связью локальных зон, таких как вокзалы, аэропорты, а также для развертывания оперативных радиосетей в зонах ЧС.

Здесь БС - базовая станция; НС - носимая станция; f - частоты.

В условиях ЧС возрастает вероятность незапланированного выбывания отдельных станций сети или их элементов из строя. Такие нарушения режима работы сети влекут за собой скачкообразные изменения интенсивностей потоков в каналах связи. Таким образом, одним из важных аспектов общей проблемы управления процессами передачи сообщений в системах связи является задача мониторинга ступенчатых изменений интенсивностей информационных потоков.

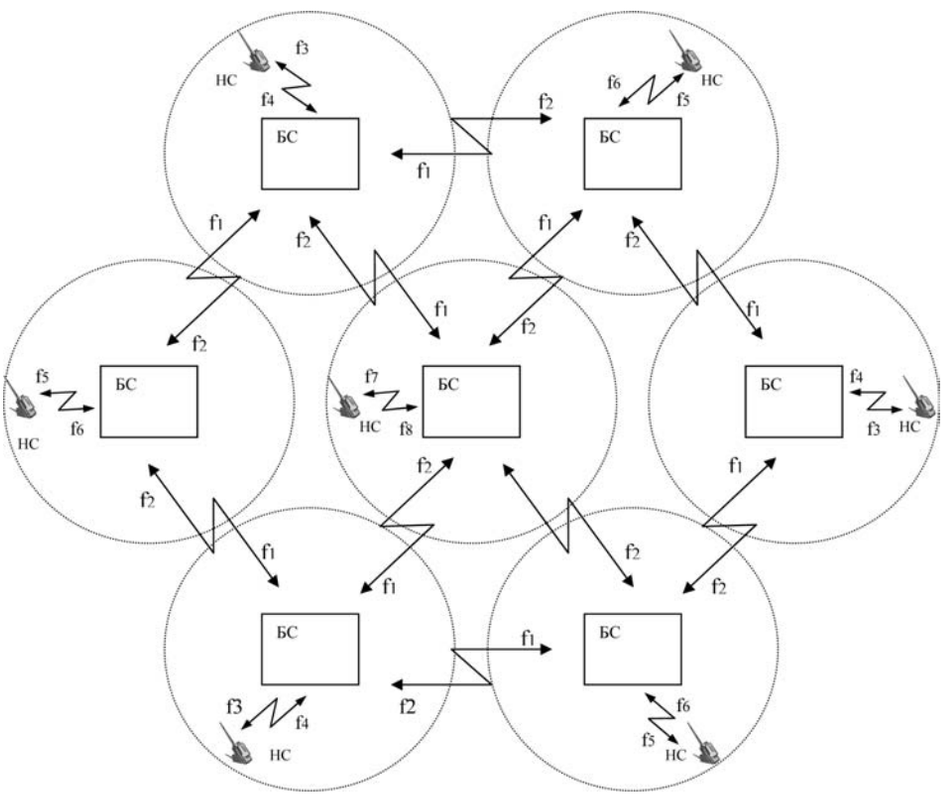


Рис. 1. Организация транкинговой радиосети

Monitoring of telecommunication networks in the conditions of emergency situations

Meleshin A.S., Khutortseva M.V.,
North-Caucasian branch of the Moscow technical university relationship and informatics

Abstract

This work consider the system of telecommunication networks monitoring at the emergency situation. The problem of the syntheses for asymptotically optimum algorithm of the joint finding step-like intensities variation (the changes means network errors) of the information flow is solved. The example is brought.

Keywords: *monitoring, discrete markov process with two conditions, information flows.*

Выявление указанных ситуаций позволяет своевременно корректировать управление информационными потоками в сети связи и минимизировать снижение эффективности процесса передачи сообщений в целом.

Известные методы выявления ступенчатых вариаций интенсивности потоков различной структуры [7,8] не могут быть непосредственно использованы для мониторинга каналов связи, поскольку не до конца учитывают вероятностную специфику процессов передачи сообщений.

Пример организации транкинговой радиосети представлен на рис. 1.

Адекватной моделью процесса передачи пакетов в канале связи может служить дискретный марковский процесс $\eta(t)$ с двумя состояниями

$\eta(t)=1$ –канал занят,

$\eta(t)=0$ – канал свободен.

Соответствующие ему вероятностные характеристики имеют вид:

$$P\{\eta(t+\Delta T)=1/\eta(t)=0\}=\pi_{01}=1-\pi_{00}, \quad (1)$$

$$P\{\eta(t+\Delta T)=0/\eta(t)=1\}=\pi_{10}=1-\pi_{11}, \quad (2)$$

$$\pi_{00}=P\{\eta(t+\Delta T)=0/\eta(t)=0\}=\frac{\beta}{\widetilde{\alpha}+\beta}+\frac{\widetilde{\alpha}}{\widetilde{\alpha}+\beta}e^{-(\widetilde{\alpha}+\beta)\Delta t}, \quad (3)$$

$$\pi_{11}=P\{\eta(t+\Delta T)=1/\eta(t)=1\}=\frac{\widetilde{\alpha}}{\widetilde{\alpha}+\beta}+\frac{\beta}{\widetilde{\alpha}+\beta}e^{-(\widetilde{\alpha}+\beta)\Delta t}, \quad (4)$$

где $\beta>0$ – параметр, характеризующий распределение длительностей передаваемых пакетов, полагаемое экспоненциальным; $\widetilde{\alpha}>0$ – интенсивность следования пакетов; $\Delta t<<1$.

Определим для интервала времени $[0,T]$ две гипотезы:

$$h_0:\widetilde{\alpha}=\alpha \ \ \forall t, \quad t\in[0,T]- \quad (5)$$

– гипотеза, соответствующая отсутствию скачка интенсивности информационного потока;

$$h_1:\widetilde{\alpha}=\begin{cases}\alpha, & \text{при } 0\le t<\theta_H\\ \alpha+\Delta\alpha, & \text{при } \theta_H\le t<T\end{cases}- \quad (6)$$

– гипотеза, соответствующая наличию такого скачка.

Здесь θ_H – случайная величина с априорной плотностью вероятности

$$w_{pr}^{h_1}(\theta)=w_{pr}(\theta/h_1). \quad (7)$$

Зададим для каждой гипотезы априорную вероятность

$$p_{h_0}=P\{\theta_H\notin[0,T]\}, \quad (8)$$

$$p_{h_1}=P\{\theta_H\in[0,T]\}. \quad (9)$$

Рассмотрим задачу синтеза алгоритма проверки гипотезы h_1 против альтернативы h_0 и в случае принятия h_1 – оценивания момента времени θ_H возникновения скачка интенсивности (6) процесса $\eta(t)$.

Введем следующие обозначения: $\bar{t}_i$ – момент появления $i-$го пакета, t_i – момент завершения его передачи. Здесь $i=\overline{1,k}$, причем $t_0<\bar{t}_1<t_1<\bar{t}_2<t_2<...<\bar{t}_k<t_k=T$. Далее полагается, что $t_0=0$.

Рассмотрим гипотезу $h_0(\theta_H\notin[0,T])$.

Функция правдоподобия для $[t_0,\bar{t}_1]$, где $\bar{t}_1-t_0=T_{1П}$ – длительность первой паузы, имеет вид [10]

$$P_{1П}=\alpha e^{-\alpha T_{1П}}\tau+O(\tau), \quad (10)$$

где $\tau<<1-$ длительность элементарного интервала времени, непосредственно примыкающего к $\bar{t}_1$.

Применительно к интервалу времени, связанному с передачей первого пакета $(\bar{t}_1,t_1]$, где $t_1-\bar{t}_1=T_{1C}$, получаем

$$P_{1C}=\beta e^{-\beta T_{1C}}\tau+O(\tau). \quad (11)$$

С учетом (10), (11) функционал правдоподобия, соответствующий гипотезе h_0 приобретает вид:

$$P_{h_0}=(\alpha\beta)^k e^{-\beta\sum_{i=1}^{k}T_{1C}-\alpha\sum_{i=1}^{k}T_{1П}}\tau^{2k}+O(\tau^{2k}). \quad (12)$$

Рассмотрим теперь гипотезу h_1, связанную с наличием на интервале $[0,T]$ ступенчатой вариации интенсивности потока передаваемых пакетов сообщений. При этом будем полагать, что

$$\widetilde{\alpha}=\begin{cases}\alpha, & \text{при } 0\le t<\theta,\\ \alpha+\Delta\alpha, & \text{при } \theta\le t<T,\end{cases} \quad (13)$$

где θ – рассматривается как параметр, определяющий возможный момент времени ступенчатой вариации.

Применяя последовательность рассуждений, использованную при выводе (12), определим функционал правдоподобия для гипотезы h_1:

$$P_{h_1}=\alpha^k\beta^{k_1}(\alpha+\Delta\alpha)^{k_2}e^{-\beta\sum_{i=1}^{k}T_{1C}-\alpha\sum_{i=1}^{k}T_{1n}-\Delta\alpha\sum_{i=k_1+1}^{k}T_{1П}}\tau^{2k}+O(\tau^{2k}). \quad (14)$$

где k_1,k_2 – количество пакетов соответственно на $[0,\theta]$ и $(\theta,T]$; $k_1+k_2=k$.

Из (12), (14) следует выражение для отношения правдоподобия и его логарифма

$$\Lambda(T,\theta)=\lim_{\tau\to0}\frac{P_{h_1}}{P_{h_0}}=\left(1+\frac{\Delta\alpha}{\alpha}\right)^{\mu(T)-\mu(\theta)}\exp\left\{-\Delta\alpha\sum_{i=\mu(\theta)+1}^{\mu(T)}T_{iП}\right\} \quad (15)$$

$$\Lambda(T,\theta)=\ln\left(1+\frac{\Delta\alpha}{\alpha}\right)\left[\mu(T)-\mu(\theta)\right]-\Delta\alpha\sum_{i=\mu(\theta)+1}^{\mu(T)}T_{iП}. \quad (16)$$

Здесь под $\mu(t)$ понимается процесс счета передаваемых пакетов, причем $\mu(\theta)=k_1,\mu(T)-\mu(\theta)=k_2$.

Применение соотношений (15), (16) на практике весьма затруднительно, поскольку связано с необходимостью фиксации интервалов времени, соответствующих паузам между передаваемыми пакетами. Задача может быть существенно упрощена, если воспользоваться асимптотической закономерностью, рассмотренной, например, в

$$P\left\{\left|\frac{\sum_{i=k_1+1}^{k}T_{iП}}{\sum_{i=k_1+1}^{k}T_i}-\frac{\beta}{\alpha+\Delta\alpha+\beta}\right|>\varepsilon\right\}\to0, \quad k_2\to\infty, \quad (17)$$

где $T_i = T_{iП} + T_{iC}, \quad \varepsilon > 0.$

Из сходимости по вероятности (17) для (15), (16) следуют асимптотические равенства

$$\Lambda(t,\theta) \cong \Lambda^a(t,\theta) = \left(1+\frac{\Delta\alpha}{\alpha}\right)^{\mu(T)-\mu(\theta)} \exp\left\{-\frac{\Delta\alpha\beta}{\alpha+\Delta\alpha+\beta}(T-\theta)\right\}, \tag{18}$$

$$\lambda^a(t,\theta) = \ln\Lambda^a(t,\theta). \tag{19}$$

Соотношения (18), (19) могут быть интерпретированы для текущего времени путем замены $T \to t$ при условии, что $\theta \le t$.

Таким образом, алгоритм принятия решения о наличии или отсутствии скачка интенсивности определяется соотношением

$$\hat{\lambda}^a = ln\int_0^t \Lambda^a(t,\theta) w_{pr}^{h_1}(\theta)d\theta\Big|_{t=T} \begin{cases} > \ln\dfrac{p_0}{p_1} \to h_1, \\ \le \ln\dfrac{p_0}{p_1} \to h_0. \end{cases} \tag{20}$$

Формирование оценки при равномерной структуре априорного распределения $w_{pr}^{h_1}(\theta)$ может быть проведено по критерию максимального правдоподобия

$$\theta^*(t) = \arg\max_{\theta}\left\{\lambda^a(t,\theta), \theta \le t, t \in [0,T]\right\} \tag{21}$$

В среде MathCAD было проведено численное моделирование синтезированных алгоритмов (20), (21). Рассматривалась передача $N = 1000$ пакетов, при этом интервал анализа определялся временем завершения передачи последнего пакета $T = t_N$. Решение задачи проводилось в безразмерном времени $\bar{t} = \dfrac{t}{t_N}$ применительно к безразмерной величине $\bar{\theta}_И = \dfrac{\theta_И}{t_N}$ с равномерной на $[0,1]$ плотностью распределения.

Значение $\bar{\theta}_И$ привязывалось к номеру m пакета, с которого вводилось изменение интенсивности $\bar{\theta}_И = \bar{t}_{pN}$, где $p = \dfrac{m}{N}$.

Для формирования дискретного марковского процесса с двумя состояниями использовались стандартные процедуры генерирования случайных чисел с экспоненциальным распределением.

Примерный вид процесса счета $\mu(\bar{t})$ при $p = 0.4, \bar{\alpha} = 10t_N$, $\bar{\beta} = 100t_N, \Delta\bar{\alpha} = 15t_N$, где $\bar{\alpha}, \bar{\beta}, \Delta\bar{\alpha}$ – приведенные к $[0,1]$ параметры, представлен на рис. 2.

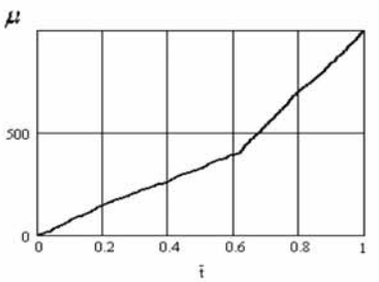


Рис. 2

Он соответствует увеличению интенсивности следования пакетов в 2.5 раза в момент времени $\bar{\theta}_И = \bar{t}_{400}$.

Эволюция во времени зависимости $\lambda^a(\bar{t},\bar{\theta})$ для $\bar{t} = 0, \quad \bar{t}_{0.7N}, \ \bar{t}_{0.85N}, \ \bar{t}_N = 1$ показана на рис. 3.

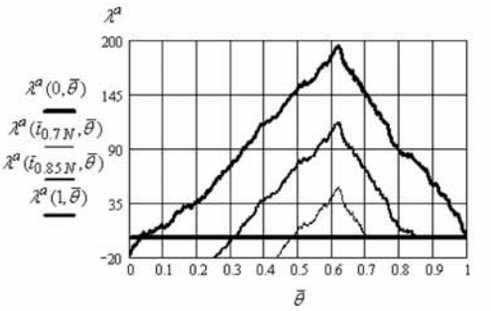


Рис. 3

Она отражает последовательность формирования экстремума логарифма асимптотического отношения правдоподобия, лежащего в основе определения оценки (21).

На рисунке 4 представлен фрагмент зависимости от времени логарифма усредненного асимптотического отношения правдоподобия (20).

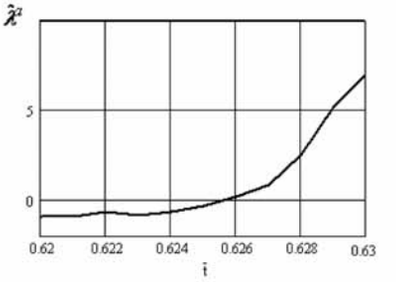


Рис. 4

Превышение нулевого порога, соответствующего случаю равновероятных гипотез, происходит при $\bar{t}_{\text{пор}} \cong 0.6255$, что примерно соответствует прохождению после скачка интенсивности $\Delta\mu \cong 14$ пакетов.

Зависимость оценки $\bar{\theta}^*$ момента ступенчатой вариации от времени проиллюстрирована на рис. 5.

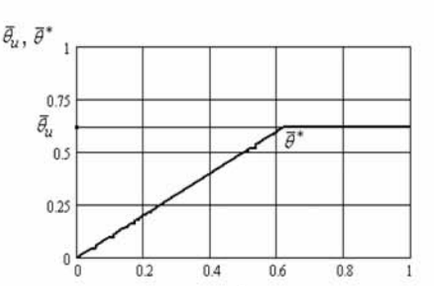


Рис. 5

Значение $\bar{\theta}^*(\bar{t})$ после $\bar{t} = \bar{t}_{\text{пор}}$ практически не меняется и для конца интервала анализа $\bar{\theta}^*(\bar{t}_N) = 0.619$.

Таким образом, в работе проведен синтез асимптотически оптимального алгоритма обнаружения ступенчатых вариаций интенсивности потока сообщений и оценивания момента времени его наступления. Его реализация является более простой по сравнению с аналогичными алгоритмами, построенными на основе (15), (16) за счет перехода к непрерывной временной координате и отсутствия необходимости измерения длительности пауз между пакетами.

Численные исследования показали работоспособность предложенного подхода и возможность его использования в задачах мониторинга каналов связи в зонах ЧС.

Литература

1. *Лазарев В.Г., Лазарев Ю.В.* Динамическое управление потоками информации в сетях связи. – М.: Радио и связь, 1983. – 216 с.
2. *Кульгин М.* Технология корпоративных сетей. Энциклопедия. – Санкт-Петербург: Питер, 1999. – 700 с.
3. Помехоустойчивость и эффективность систем передачи информации / Под ред. А.Г.Зюко. – М.: Радио и связь, 1985. – 275 с.
4. *Хуторцев В.В, Хуторцева М.В.* О синтезе итерационной процедуры оптимизации виртуальных каналов телекоммуникационных систем по критерию минимума вероятности занятости // Автоматика и вычислительная техника, 2008. –№6. – С. 66-73
5. *Хуторцева М.В.* Динамическое программирование виртуальных каналов телекоммуникационных систем по критерию минимума вероятности занятости // труды конференции «ИНФОКОМ-2008». – С. 47-56.
6. *Хуторцев В.В., Хуторцева М.В.* О мониторинге ступенчатых вариаций интенсивностей потоков сообщений в телеком-муникационных системах // Телекоммуникации, 2009. – №1. – С. 2-6.
7. *Клигене Н., Телькснис Л.* Методы обнаружения моментов изменения свойств случайных процессов // Автоматика и телемеханика, 1983. – №10. – С.5-56.
8. *Галун С.А., Трифонов А.П.* Обнаружение и оценка момента изменения интенсивности пуассоновского потока // Автоматика и телемеханика, 1982. – №6. – С.95-105.
9. *Тихонов В.И., Миронов М.А.* Марковские процессы. – М.: Сов. Радио, 1977. – 488 с.
10. *Тихонов В.И., Харисов В.Н.* Статистический анализ и синтез радиотехнических устройств и систем. – М.: Радио и связь, 1991. – 608 с.
11. *Ширяев А.Н.* Вероятность. – М.: Наука, 1980. – 576 с.

Некоторые подходы к системному анализу процессов управления современными мультисервисными сетями связи

Основанием системного анализа процессов управления является системный подход. Системный подход – это подход, при котором мультисервисная сеть связи как объект управления рассматривается как совокупность взаимосвязанных элементов (компонентов), имеющая выход, цель, входы и ресурсы, связь с внешней средой, обратную связь. В соответствии с этим мультисервисную сеть связи как объект управления целесообразно представить в виде модели.

Ключевые слова: *мультисервисная сеть, процесс, управление, системный анализ, объект управления.*

Буренин А.Н. , Легков К.Е., Мясникова А.И.,
Военно-космическая академия имени А.Ф.Можайского

Some approaches to systems analysis of administrative processes by the modern multiservice communication networks

Burenin A.N., Legkov K.E., Myasnikova A.I.,
Military space academy of a name of A.F.Mozhaysky

Abstract
The base of systems analysis of administrative processes is the systems concept. The systems concept ? is approach in case of which a multiservice communication network as the control object is considered as the set of interdependent elements (components) having an output, the purpose, inputs and resources, communication with an external environment, back coupling. According to it as a control object it is expedient to provide a multiservice communication network in the form of model.

Keywords: *multiservice network, process, control, systems analysis, control object.*

Современная мультисервисная сеть связи как сложный объект управления характеризуется некоторыми чертами, которые требуется учитывать при управлении. Все эти обстоятельства приводят к тому, что цели управления сетью в полной мере никогда не будут достигнуты и для разрешения неопределенностей требуется проведения системного анализа процессов управления [1, 2].

Учитывая особенности современной мультисервисной сети связи [3], которая строится в соответствии с концепцией сетей следующего поколения (NGN), целесообразно предложить следующую структуру системного анализа процессов управления.

Системный подход и характеристики процессов управления. Основанием системного анализа процессов управления является системный подход. Системный подход — это подход, при котором мультисервисная сеть связи как объект управления рассматривается как совокупность взаимосвязанных элементов (компонентов), имеющая выход, цель, входы и ресурсы, связь с внешней средой, обратную связь. В соответствии с этим мультисервисную сеть связи как объект управления целесообразно представить в виде модели, изображенной на рис. 1.

Если Z_c — воздействие среды на сеть (так называемый неуправляемый наблюдаемый вход), отражающий в т.ч. и требования пользователей сети с различным уровнем сервиса, управление сетью U_c (управляемые входы), S_c — состояние сети (выход), то зависимость между ними можно представить следующим выражением:

$$S_c = F(U_c Z_c), \qquad (1)$$

где F — оператор, связывающий вход Z_c (воздействие среды), управление U_c и выход S_c (состояние сети).

При управлении важна цель C_c, которая определяет, какой должна быть мультисервисная сеть связи с точки зрения управления. Обычно цель формулируется в виде условного вектора цели

$$C_c = (c_1,\ldots,c_p). \qquad (2)$$

Все $(c_1,\ldots,c_p)$ определяют вполне определенные функции, которые, в принципе, могут носить различный характер, однако их форму целесообразно свести к одной из трех:

$$c_i = a_i;\ \ c_j \geq (\leq) b_j;\ \ c_l \to \min(\max) \qquad (3)$$

Рис. 1. Модель мультисервисной сети связи в рамках системного подхода

Обычно информация о сети для системы управления всегда является неполной. Это явление можно описать наличием ненаблюдаемого входа сети, на который поступают возмущения $\mathfrak{I}_c$, характеризующие все ненаблюдаемые внешние и внутренние факторы в сети, влияющие на ее состояние. Ненаблюдаемые возмущения $\mathfrak{I}_c$ не могут быть измерены, относительно них обычно выдвигаются лишь определенные предположения (к ним могут быть отнесены, например, всевозможные необнаруженные воздействия различных нарушителей).

Располагая информацией о состоянии среды, сети и цели, можно представить управление как

$$\mathbf{U}_c = \mathbf{F}^*\left(\mathbf{Z}_c\mathbf{S}_c\mathbf{C}_c\right), \quad (4)$$

где $\mathbf{F}^*$ оператор, отображающий информацию о среде, сети и цели в управление $\mathbf{U}_c$.

Все ситуации, которые могут складываться в процессе управления мультисервисной сетью связи, можно подразделить на управляемые, при которых заданная цель $\mathbf{C}_c$ всегда достигается, и неуправляемые, когда эта цель $\mathbf{C}_c$ не достигается.

Будем называть сеть абсолютно управляемой, если каждая ситуация управляема, т.е. цель управления всегда достигается. Это означает, что для любого контролируемого состояния среды $\mathbf{Z}_c$, любого неконтролируемого входа $\mathfrak{I}_c$ и для любой цели $\mathbf{C}_c$ всегда найдется такое управление $\mathbf{U}_c$, которое переведет сеть в требуемое состояние. Целесообразно ввести понятия частичной или относительной управляемости сети.

Реализовать цели управления можно только соответствующим изменением состояния $\mathbf{S}_c = \mathbf{F}\left(\mathbf{U}_c\mathbf{Z}_c\right)$ при выборе определенного управления $\mathbf{U}_c$. Это приводит к экстремальной задаче:

$$\mathbf{Q}\left(\mathbf{Z}_c,\mathbf{S}_c\right) \to \min_{\mathbf{U}_c} \quad (5)$$

Решением этой экстремальной задачи является некоторое управление $\mathbf{U}_c^*$, являющееся оптимальным управлением. Задача требует минимизации показателя эффективности Q путем подбора соответствующего управления.

При решении существенным является вид $\mathbf{F}$: является ли $\mathbf{F}$ функцией или оператором. При этом получаются две различные задачи оптимизации, которые решаются принципиально разными методами,

Так если на каждом цикле управления мультисервисную сеть связи можно рассматривать как квазистатический объект (т.е. состояние сети внутри каждого цикла управления можно считать стационарным случайным вектором), для которого $\mathbf{F}$ является функцией, то задача синтеза управления сетью в этом случае заключается в минимизации функций $q_l(\mathbf{U}_c\mathbf{Z}_c)\ \forall l = 1,...,k_3)$ путем изменения q параметров $u_1,...,u_q$ управления $\mathbf{U}_c$. Задачи такого класса являются задачами математического программирования и характерны при организации управления статическими (квазистатическими) для каждого цикла управления мультисервисными сетями связи.

Если мультисервисную сеть связи внутри цикла управления нельзя рассматривать как квазистатический объект, а только как динамический объект, для которого F является оператором, то в этом случае управление $\mathbf{U}_c$ представляет собой векторную функцию времени $\mathbf{U}_c(t)$, и задача переходит в разряд вариационных задач. Таким образом, управление сетью как динамическим объектом, сводится к решению определенной вариационной задачи.

Логическая структура процессов: объект и субъект управления. Выполнение целей $\mathbf{C}_c = (c_1,...,c_p)$, поставленных перед системой управления, должно гарантировать функционирование мультисервисной сети связи с требуемой эффективностью. Управление мультисервисной сетью связи будем считать эффективным, если оно обеспечивает требуемую эффективность функционирования самой сети в условиях воздействия на нее и систему управления сетью различных естественных и преднамеренных возмущений и помех (в т.ч. программно-аппаратных атак). Иными словами эффективность управления определяется эффективностью и устойчивостью управляемой мультисервисной сети. Под эффективностью мультисервисной сети связи будем понимать меру соответствия сети своему назначению. Количественно эффективность оценивается с помощью показателей эффективности, в роли которых могут выступать ее характеристики качества.

Из всей совокупности возможных показателей эффективности обычно выделяют основной показатель эффективности (ОПЭ), позволяющий в наибольшей степени оценить способность мультисервисной сети связи выполнять возложенные на нее задачи. Поэтому возникает задача: из совокупности характеристик качества сети выбрать такую характеристику (или группу характеристик), которая бы в наибольшей степени удовлетворяла определению ОПЭ.

Особенности мультисервисных сетей связи приводят к необходимости корректировки общепринятых подходов к выбору тех или иных показателей эффективности их функционирования. Так в качестве временных показателей эффективности целесообразно применять случайное t_{serv} или среднее t^*_{serv} время обслуживания требований, которые включают на отдельных фрагментах мультисервисной сети связи время задержки пакета (кадра, ячейки), время установления (проключения) виртуального или физического соединения, время передачи единицы информации по каналу или тракту. Также в качестве показателя эффективности мультисервисной сети связи может быть выбрана вероятность $P(t_{serv} \le t_d)$ обслуживания требования (доставки, задержки) сообщения (пакета, кадра, успешного установления виртуального или физического соединения и т.д.) за заданное t_d (допустимое) время. Будем считать, что мультисервисная сеть удовлетворяет заданным требованиям по эффективности, если $t_{serv} \le t_d$, $t^*_{serv} \le t_{servd}$, $P(t_{serv} \le t_d) \ge P_d$.

Наличие различным возмущений (воздействий) в процессе функционирования сети может привести к снижению эффективности функционирования мультисервисной сети связи или даже к срыву выполнения целевых задач, стоящих перед ней.

Естественно, что основной целью функционирования мультисервисной сети связи является предоставление пользователям всех необходимых услуг связи с требуемым качеством. Если эффективность функционирования мультисервисной сети связи в течение заданного времени обеспечиваются с вероятностью не меньшей требуемой, несмотря на целый ряд воздействий на нее, то функционирование сети признается устойчивым, а управление ею – эффективным.

В процессе организации управления реальной мультисервисной сетью связи определяющее значение будут иметь существующие в сети типы неуправляемостей, особенно перекрестных неуправляемостей (зависящих сразу от двух или трех факторов $\mathbf{Z}_c, \Im_c, \mathbf{C}$), определяющих потенциальную эффективность управления сетью.

Для разрешения возникающих противоречий, связанных с тем, что нередко невозможно отделить $\mathbf{Z}_c$ от $\Im_c$, и не существует механизмов учета этого при синтезе управления мультисервисной сетью связи, целесообразно, в рамках системного анализа, рассмотреть формальную постановку задач управления сетью, рис. 2.

Пусть вектор $\overline{\mathbf{S}}_n(t)$ определяет состояние мультисервисной сети связи в текущий момент времени *t* в том смысле, что в последующие моменты времени $\Theta > t$ вектор $\overline{\mathbf{S}}_n(\Theta)$ зависит только от $\overline{\mathbf{S}}_n(t)$ и управляющих воздействий на сеть.

Система управления «наблюдает» за мультисервисной сетью связи, однако из-за воздействия вектора помех $\overline{\mathbf{\Pi}}(t)$ доступен для измерения не сам вектор $\mathbf{S}_n(t)$, а некоторый вектор наблюдения $\overline{\mathbf{X}}_r(t)$.

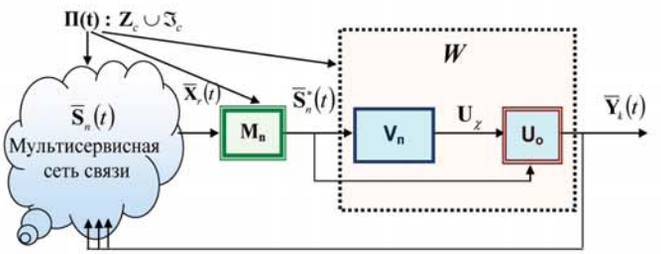


Рис. 2. Формальная постановка задачи управления

Будем считать, что размерности векторов $\overline{\mathbf{S}}_n(t)$ и $\overline{\mathbf{X}}_r(t)$, а также качественный состав их элементов совпадают (т.е. $n = k$). Тогда оценка вектора $\overline{\mathbf{S}}_n(t)$ (вектор $\overline{\mathbf{S}}_n^*(t)$) может быть осуществлена (оператор M_n) статистическими методами обработки вектора $\overline{\mathbf{X}}_r(t)$. При этом, процесс управления мультисервисной сетью связи состоит в том, что каждому вектору $\overline{\mathbf{S}}_n^*(t)$ должен соответствовать определенный вектор управления $\mathbf{U}_\chi(t)\ \forall \chi \le n$ и соответствующий ему вектор управляющих воздействий $\mathbf{Y}_k(t) = [y_1(t), \cdots, y_k(t)]$, которые могут быть выработаны по соответствующей процедуре управления, предусматривающей обеспечение экстремума некоторого показателя эффективности (задаваемого соответствующим функционалом), т.е. обеспечение выбранного критерия эффективности:

$$\Phi\left[t, \overline{\mathbf{S}}_n^*(t), \mathbf{W}\right] \to \min_{\mathrm{w}}, \qquad (6)$$

где $\Phi\left[t, \overline{\mathbf{S}}_n^*(t), \mathbf{W}\right]$ определенный функционал, задающий выбранный показатель эффективности.

При управлении с обратной связью соответствие $\mathbf{Y}_k(t) = [y_1(t), \cdots, y_k(t)]$ определенной оценке состояния $\overline{\mathbf{S}}_n^*(t)$ мультисервисной сети связи обеспечивает *W* – оператор управления, в функциональном плане представляющий собой совокупность подоператоров планирования $\mathbf{V}_\Pi$ и оперативного управления $\mathbf{U}_o$.

В плане декомпозиции оператора *W* по уровням архитектуры системы управления, его можно представить состоящим из подоператоров управления организацией (планированием) связи $\mathbf{W}_{nc}$, услугами $\mathbf{W}_{serv}$, телекоммуникационными сетями $\mathbf{W}_{netw}$, оборудованием сети (сетевыми элементами) $\mathbf{W}_{ne}$, каждый из которых включает подоператоры планирования и оперативного управления, т.е. $\mathbf{W}_{nc} = \{\mathbf{V}_{nc}, \mathbf{U}_{nc}\}$, $\mathbf{W}_{serv} = \{\mathbf{V}_{serv}, \mathbf{U}_{serv}\}$, $\mathbf{W}_{netw} = \{\mathbf{V}_{netw}, \mathbf{U}_{netw}\}$, $\mathbf{W}_{ne} = \{\mathbf{V}_{ne}, \mathbf{U}_{ne}\}$.

Чтобы описать АСУ сетью множеству центров (пунктов) управления *i*-го уровня можно поставить в соответствие некоторое множество чисел натурального ряда, которое соответствует множеству индексов *i*-го уровня иерархии системы управления: $I_i = \{1, 2, \ldots, M_i\}$, где M_i - число одноуровневых центров управления на *i*-м уровне иерархии.

Каждый *l*-й центр управления *i*-го уровня АСУ характеризуется множеством векторов состояния $S_{il}^u = \{\mathbf{s}_{il}^{hu}\}$ размерности h_{il}, множеством векторов локальных выходных переменных $Y_{il}^u = \{\mathbf{y}_{il}^{au}\}$ размерности a_{il}, по которым производится управление, множеством векторов обобщенных выходных переменных $B_{il}^u = \{\mathbf{b}_{il}^{bu}\}$ размерности *b*, выдаваемых на *j*-й центр управления (*i*+1)-го уровня, множеством векторов обобщенных выходных переменных $B_{i-1,l}^u = \{\mathbf{b}_{i-1,l}^{\varepsilon}\}$, поступающих в *l*-й центр управления от подчиненных ему центров управления (*i*-1)-го уровня иерархии, множеством векторов самоуправления $U_{il}^{lu} = \{\mathbf{u}_{il}^{qu}\}$ размерности *q*, множеством векторов управления $U_{il}^{ju} = \{\mathbf{u}_{il}^{ru}\}$ размерности *r*, с помощью которого *j*-й центр управления (*i*+1)-го уровня иерархии АСУ осуществляет управление *l*-м центром управления *i*-го уровня, множеством векторов управления $U_{i-1,l}^u = \{\mathbf{u}_{i-1,l}^{xu}\}$, с помощью которого *l*-й центр управления *i*-го уровня иерархии АСУ осуществляет управление подчиненными центрами управления (*i*-1)-го уровня.

Литература

1. Tsisa.ru— ресурс о теории систем и системном анализе.

2. Системный анализ. Википедия.

3. *Москвитин В.Д.* От Взаимоувязанной сети связи к Единой сети электросвязи России // Вестник связи, 2003. - №8. – С.33-48.

4. *Легков К.Е.* Управление ресурсами информационных систем специального назначения при построении сетецентрической системы управления на основе радиосетей нового поколения // T-Comm: Телекоммуникации и транспорт, 2012, №10. – С. 60-63.

5. *Легков К.Е.* Беспроводные локальные сети IEEE 802.11: механизм распределения скоростей // T-Comm: Телекоммуникации и транспорт, 2010, №5. – С. 17-19.

Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями

В соответствии с особенностями построения и условиями функционирования инфокоммуникационных сетей специального назначения (ИКС СН), с учетом требований стандартов по организации сетей управления телекоммуникациями (TMN) и организации систем сетевого управления (NMS), предлагаются различные варианты организации управляющей сети (УС) для автоматизированной системы управления (АСУ ИКС СН) на базе стандартной защищенной технологии в составе протокола IPv6, приводятся варианты математического описания УС, включающие вероятностные модели, модели массового обслуживания, приводится математическая модель передачи управляющей информации между центрами управления АСУ ИКС СН, позволяющая получить оценки вероятностно-временных характеристик УС.

Ключевые слова: *управляющая сеть, система управления, инфокоммуникационная система, система управления, математическая модель.*

Легков К.Е., Буренин А.Н.,
Военно-космическая академия имени А.Ф. Можайского

Models of the organization of the information managing director of a network for management system the modern infocommunication networks

Legkov K.E., Burenin A.N.,
Military space academy of name A.F. Mozhaisky

Abstract

According to features of creation and operating conditions of infocommunication networks of a special purpose, taking into account requirements of standards for the organization of networks of telecommunication management (TMN) and the organization of systems of network control (NMS), different options of the organization of the controlling network (CN) for an automated control system are offered on the basis of the standard protected technology as a part of the IPv6 protocol, are brought versions of the mathematical description the CN, including probability models, waiting line models, is given a mathematical model of transmission of control data between centers automated control system, allowing to receive estimates of probable time response characteristics the CN.

Keywords: *controlling network, management system, infocommunication system, management system, mathematical model.*

Основой современных систем связи различных ведомств и крупных госкорпораций являются инфокоммуникационные сети специального назначения (ИКС СН), функционирование которых осуществляется в достаточно сложных и неблагоприятных условиях обстановки [1], что требует организации достаточно четкого и устойчивого управления ими в реальном масштабе времени.

Современные ИКС СН строятся в соответствии с концепцией глобальной информационной инфраструктуры (GII) [2] на базе широкого применения современных информационных и телекоммуникационных технологий и технологий управления, рис.1.

Несмотря на сложность обеспечения функционирования ИКС СН в сложных условиях функционирования, необходимо обеспечить передачу требуемого объема информации с гарантированным качеством от индивидуальных или корпоративных пользователей в условиях возможных интенсивных воздействий на средства сети и оборудование ее узлов. Это можно обеспечить только при наличии гибкой АСУ ИКС СН, реализующей эффективные методы управления, и при организации качественного обмена управляющей информацией между пунктами управления (ПУ). Этот обмен управляющей информацией должна обеспечить (в соответствии с рекомендациями МСЭ-Т по TMN, серия М.30**) специальная выделенная сеть управления, учитывающая специфику решения задач управления ИКС СН.

Так как архитектура современных ИКС СН, построенных в соответствии с концепцией GII, содержит три основных уровня (рис. 1), то управление ею также целесообразно декомпозировать на три уровня управления: управление инфраструктурным уровнем, управление промежуточным уровнем, управление базовым уровнем ИКС СН, на каждом из которых управление осуществляется по пяти основным задачам управления, к которым относятся задачи управления производительностью уровня, безопасностью, структурой и адресацией, ресурсами уровня и сбойными ситуациями [2].

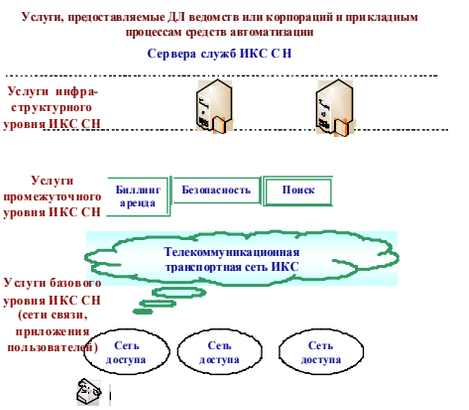


Рис. 1. Архитектура современных ИКС СН

Каждый уровень архитектуры ИКС СН [2] представляет собой сеть или совокупность сетей:

— инфраструктурный уровень представляет собой совокупность сетей услуг;

— промежуточный уровень представляет собой совокупность сетей услуг middleware (услуги безопасности, биллинга, аутентификации, поиска);

— базовый уровень — совокупностью транспортной сети, сетей доступа и сетей традиционной связи.

Значительная часть вышеперечисленных групп управления осуществляется на основе передачи соответствующих документов с использованием телекоммуникационных служб электронная почта и файловый обмен как по сети управления, так по самой управляемой ИКС СН, путем выделения специального ресурса. При любом варианте управляющей сети она, как правило, организуется путем наложения защищенной IP-сети на транспортную основу с применением маршрутизаторов центров управления), рис.2.

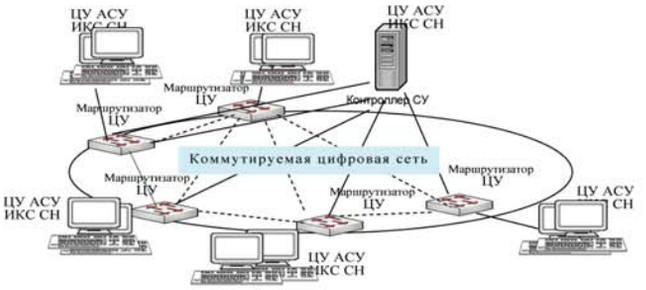


Рис. 2. Топология управляющей сети АСУ ИКС СН

При построении IP-сети поверх коммутируемой цифровой сети (например, сети ISDN) между слоем коммутируемых цифровых каналов и слоем IP существует цифровая сеть. Это, при соответствующей корректировке вероятностно-временных характеристик, справедливо и при организации IP-сети поверх сети FR, ATM и пр.

Каждый порт маршрутизатора центра управления сетью должен поддерживать интерфейс соответствующего канала в качестве конечного узла. После того как каналы установлены, маршрутизаторы могут пользоваться ими как физическими, посылая данные порту соседнего (по отношению к виртуальному каналу) маршрутизатора. В сети образуется сеть выделенных каналов с собственной топологией.

Подсеть коммутируемых каналов прозрачна для IP-маршрутизаторов сети управления, они ничего не знают о физических связях между портами коммутаторов сети. При этом IP-сеть является наложенной по отношению к этой сети. А сам сеанс организации того или иного соединения для повышения устойчивости управления ИКС СН осуществляется только на время обмена управляющей информацией, что существенно повышает скрытность процессов управления.

Для оценки вероятностно-временных характеристик передачи управляющей информации рассмотрим схему ее организации при наложенной сети, рис. 3.

Для обеспечения защищенной передачи управляющей информации целесообразно применять криптомаршрутизатор (КМ), который реализует протокол IP-sek (защищенный подпротокол протокола IPv6) в транспортном или туннельном вариантах. В рассматриваемом варианте для каждого цикла управления ИКС СН сеть управления может быть представлена совокупностью двухполюсных сетей между взаимодействующими центрами управления сетью.

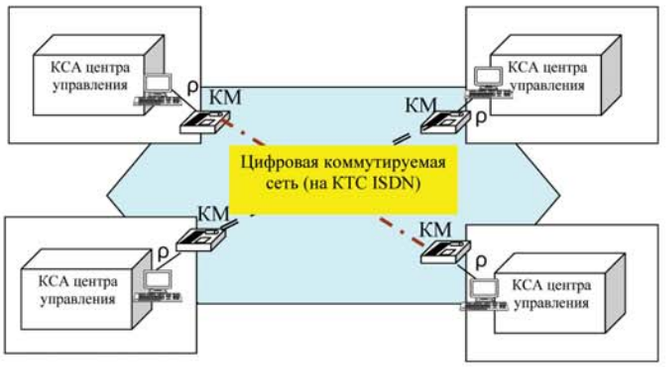


Рис. 3. Двухполюсная декомпозиция процедур обмена управляющей информацией между ПУ АСУ ИКС СН

В цифровой сети используется метод коммутации цифровых каналов, при котором информация (в виде IP-пакетов) вводится в сеть только после установления соединения, т.е. передача массива IP-пакетов возможна лишь после того, как образован сквозной канал между вызываемым и вызывающим КМ. Несомненным преимуществом такой организации является возможность немедленного (с задержкой на время установления соединения) обмена информацией между двумя КМ. В сети с коммутацией каналов прохождение срочной информации, обладающей высшим приоритетом, происходит сравнительно быстро, однако этот эффект достигается путем прерывания каналов для информации с низкой категорией приоритета. Естественно, управляющая информация обладает высшим приоритетом.

Эффективность метода коммутации каналов в цифровой коммутируемой сети существенно зависит от соотношения между средним временем передачи одного массива IP-пакетов $\overline{t}_{n1}$ и временем установления соединения $\overline{t}_y$. В современной ISDN сети всегда выполняется условие [3]:

$$\overline{t}_{n1} > \overline{t}_y \qquad (1)$$

Среднее время установления соединения $\overline{t}_y$ на k участков равно $\overline{t}_y = k\overline{t}_{к1}$, где $\overline{t}_{к1}$ – среднее время проключения (коммутации) цифрового канала между двумя соседними узлами ISDN. Случайное время $t_{к1}$ в ISDN сети имеет распределение близкое к нормальному с дисперсией незначительной величины [3], которой можно пренебречь. Поэтому можно считать $t_{к1} \approx \overline{t}_{к1}$.

Случайное число транзитных участков в установленных соединениях цифровых каналов в ISDN сети, как правило, имеет распределение близкое к равномерному. Это объясняется тем фактом, что в ISDN сети применяются алгоритмы динамического управления сетью.

Поэтому можно считать, что случайное время t_y также имеет равномерное распределение со средним значением $\overline{t}_y$.

Тогда среднее время доставки IP-пакета в наложенной управляющей сети можно определить из выражения:

$$\overline{t}_{\text{п}} = \frac{Q_{\text{п}}}{v_{эф}} + \overline{t}_{к2} + \overline{t}_{з}, \quad (2)$$

где $\overline{t}_{з}$ – среднее время задержки пакета в КМ; $\overline{t}_{к2}$ – среднее время обработки заголовка IP-пакета с обращением к маршрутной таблице; $Q_{\text{п}}$ и $v_{эф}$ – соответственно объем IP-пакета и эффективная скорость передачи его по установленному цифровому каналу.

Средне время задержки пакета в КМ $\overline{t}_{з}$ можно определить, если описать КМ в виде системы массового обслуживания (СМО) [4, 5], предполагая, что пакеты, поступающие из центров управления сетью, образуют самоподобный поток с конечным числом источников, при этом значение $\overline{t}_{з}$ определится выражением:

$$\overline{t}_{з} = \frac{Q_{\text{п}} \sum_{k=1}^{m} \frac{(k-1)m!\rho^{k}}{(m-k)!}}{v_{эф}} P_0, \quad (3)$$

где ρ – нагрузка, поступающая на КМ; m – число IP-пакетов, которое может поступить за время цикла управления (определяется объемом управляющего сообщения);

$P_0 = \dfrac{1}{1 + \dfrac{m!\rho}{(m-1)!} + \sum_{k=2}^{m} \dfrac{m!\rho^{k}}{(m-k)!}}$ – вероятность того, что КМ незагружен.

Тогда среднее время доведения управляющего сообщения для каждой пары взаимодействующих комплексов средств автоматизации ЦУ АСУ ИКС СН составит:

$$\overline{t}_{\text{дус}} = \overline{t}_{y} + m\left[\overline{t}_{к2} + \frac{Q_{\text{п}}}{v_{эф}}\left(1 + \frac{\sum_{k=1}^{m} \frac{(k-1)m!\rho^{k}}{(m-k)!}}{1 + \frac{m!\rho}{(m-1)!} + \sum_{k=2}^{m} \frac{m!\rho^{k}}{(m-k)!}}\right)\right] \quad (4)$$

Отметим важное обстоятельство, что для рассматриваемой модели (одноканальной СМО), приведенные выражения справедливы в состоянии установившегося стохастического равновесия для любых законов распределения времени обслуживания [4].

Полный ряд распределения вероятностей возможных состояний отдельного КМ можно получить, вычислив вероятности этих состояний:

$$P_k = \frac{m!\rho^{k}}{(m-k)!} P_0 \quad (5)$$

При этом каждое состояние КМ будет соответствовать определенному времени задержки IP-пакета, поступающего на него. Так с вероятностью P_0 время задержки равно 0, с вероятностью P_1 время задержки равно $\dfrac{Q_{\text{п}}}{v_{эф}}$, с вероятностью P_2 время задержки составит $\dfrac{2Q_{\text{п}}}{v_{эф}}$ и т.д. С целью получения оценки вида непрерывного распределения этот ряд может быть аппроксимирован соответствующей функцией (например, взвешенной суммой экспонент).

Предложенный подход и полученные выражения могут быть использованы и при организации наложенной IP-сети на основе цифровых сетей с применением технологий FR или ATM [6], при этом изменяется только временные характеристики организации сеансов обмена управляющей информацией между ЦУ АСУ ИКС СН [7], определяемые особенностями телекоммуникационных технологий FR и ATM. Так при использовании в качестве транспортной магистральной сети ИКС СН ATM-сети время установления виртуального цифрового соединения будет определяться задаваемым режимом передачи (ABR, VBR), а также применяемым для передачи информации АСУ ИКС СН сервисом уровня адаптации ATM (AAL1, AAL2, AAL3\4 или AAL5).

На рис. 4 приведены сравнительные характеристики вероятностно-временных параметров передачи управляющей информации АСУ ИКС СН при организации транспортной основы для наложенной IP управляющей сети с использованием соответственно технологий ISDN (кривая 1), FR (кривая 2) и ATM при AAL5 (кривая 3) в зависимости от средней интенсивности потоков управляющей информации.

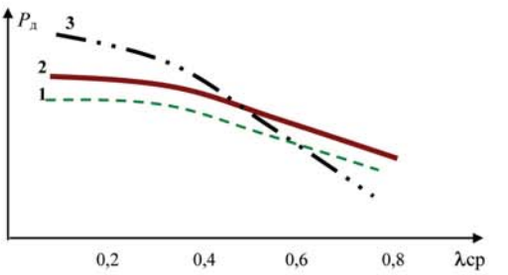


Рис.4. Вероятность своевременной доставки управляющего сообщения в управляющей сети АСУ ИКС СН

Таким образом, предложен вариант организации управляющей сети для подсистем управления телекоммуникационными сетями, основанный на наложении IP-сети на цифровую коммутируемую ISDN, FR или ATM сеть, получены и приведены основные вероятностно-временные характеристики процессов передачи управляющей информации, которые могут быть использованы для оценки эффективности управляющей сети.

Литература

1. *Бабошин В.А., Сиротенко Ф.Ф. Легков К.Е.* Алгоритм мониторинга телекоммуникационной сети специального назначения и методика ее выбора.// Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Вып.1. Ростов-на-Дону, 2011. – С. 23-26.

2. ITU-T Recommendation Y.101 (2000), Global Information Infrastructure terminology: Terms and definitions.

3. *Боккер П.* ISDN. Цифровая сеть с интеграцией служб. Понятия, методы, системы /Пер. с нем. – М.: Радио и связь, 1991. – 304 с.

4. *Клейнрок Л.* Теория массового обслуживания. – М.: Машиностроение, 1979. – 432 с.

5. *Саати Т.Л.* Элементы теории массового обслуживания и ее приложения. – М.: Сов. Радио, 1971. – 520 с.

6. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. – СПб. Питер. Изд.4. 2004. – 872 с.

7. *Буренин А.Н.* Системно-архитектурные вопросы построения автоматизированных систем управления связью // Телекоммуникационные технологии. – СПб. «Политехника». 1996. Вып.1. – С.97-112.

К вопросу о сферах безопасности вычислительных систем

В настоящее время компании и организации выбирают решения, руководствуясь требованиями к непрерывности работы, безопасности, эргономичности и стоимости. Такие технические моменты, как тактовая частота процессора и объем памяти устройств, уже не играют столь важной роли, как раньше. На современном предприятии информация хранится и обрабатывается, главным образом, на компьютерах. Если они соединены в локальную сеть, то это создает большие возможности для эффективного управления всеми процессами на предприятии. Если есть возможность использования глобальных сетей, то в пределах одного помещения можно управлять удаленными офисами и серверами предприятия. Немаловажным является вопрос безопасности вычислительных систем, который и рассмотрен в настоящей статье.

Ключевые слова: *безопасность, вычислительная система, локальная сеть, сервер, компьютер.*

Зайцева И.В.,
Ставропольский государственный аграрный университет

Spheres of computing systemssafety

Zaytseva I.V.,
Stavropol state agrarian university

Abstract

Now the companies and the organizations select decisions, being guided by requirements to a continuity of operation, safety, ergonomics and cost. Such technical moments as the clock rate of the processor and memory size of devices, any more don't play so important role as earlier. At the modern enterprise information is stored and processed, mainly, on computers. If they are connected in a local area network, it creates great opportunities for effective management of all processes at the enterprise. If there is a possibility of use of wide area networks, within one location it is possible to control remote offices and enterprise servers. The safety issue of computing systems which is considered in the present article is important.

Keywords: *safety, computing system, local area network, server, computer.*

Информационной безопасности в наше время уделяется очень большое внимание. Создана большая нормативно-теоретическая база, формальные математические методы которой обосновывают большинство понятий, формулировавшихся ранее лишь с помощью словесных описаний. Предлагается отталкиваться от подхода, разработанного при формировании этой нормативно-правовой базы, в рамках которой определяется допустимые границы решения, не заботясь о том, насколько оно эффективно или нет. Следовательно, модель безопасности и для технических и для социальных систем - это перечень ограничений, использование которых позволяет существенно снизить риски при использовании ИТ-систем [2]. При этом следует говорить именно о рисках, так как полностью обеспечить безопасность ни одни рамки и ограничения не могут, как потому что невозможно определить все возможные комбинации решений и выбрать из них, оптимальный для каждого частного случая, так и потому что не существует исчерпывающего знания. При этом разработчики систем безопасности, реализующих различные способы и методы противодействия угрозам информации, стараются максимально облегчить работу по администрированию безопасности.

Корпоративная система предприятия, как правило, охватывает все стороны его деятельности: административную, производственную, финансовую. В ней содержатся сведения, касающиеся планов, договоров, состояния материальных и финансовых потоков, данные финансового и управленческого учета. Такого рода коммерческая информация носит сугубо конфиденциальный характер, а ее утрата может оказаться критичной для работы всего предприятия. Именно поэтому организация работы пользователей с содержащейся в системе информацией требует специальных мер защиты, обеспечивающих конфиденциальность, целостность и доступность данных.

Сегодня компании и организации выбирают решения, руководствуясь требованиями к непрерывности работы, безопасности, эргономичности и стоимости. Такие технические моменты, как тактовая частота процессора и объем памяти устройств, уже не играют столь важной роли, как раньше.

На современном предприятии информация хранится и обрабатывается, главным образом, на компьютерах. Если они соединены в локальную сеть, то это создает большие возможности для эффективного управления всеми процессами на предприятии. Если есть возможность использования глобальных сетей, то в пределах одного помещения можно управлять удаленными офисами и серверами предприятия. Но элементы локальной вычислительной сети, также могут являться источниками утечки информации. Для этого большинством информационных систем используются стандартные подходы, ставшие результатом накопления разработчиками систем защиты опыта создания и эксплуатации подобных систем. Разработка системы защиты информации должна реализовывать какую-либо политику безопасности (набор правил, определяющих множество допустимых действий в системе), при этом должна быть реализована полная и корректная проверка ее условий. Существуют специальные модели безопасности - системы, функционирующие в соответствии со строго определен-

ным набором формализованных правил, и реализующие какую-либо политику безопасности.

Концептуально суть модели безопасности состоит в том, что она задает допустимые границы, ниже которых решение не может быть реализовано.

В качестве основных сфер безопасности [1] были выделены следующие:

Техническая сфера - сфера безопасности, связанная с работоспособностью, надежностью, безотказностью и т.д. технической инфраструктуры, на которой функционирует ИТ-система. Включает в себя физическую безопасность, связанную с физическими угрозами (взлома, кражи, террористического акта, пожара, наводнения и т.д.) ресурсам ИТ-системы и критичной информации.

Программная сфера - сфера безопасности, связанная с работоспособностью, надежностью, безотказностью, защитой от несанкционированного доступа и т.д. программных средств ИТ-систем.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности [5]. Они включают:

1. Мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных.

2. Мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности).

3. Мероприятия, осуществляемые при подборе и подготовке персонала системы.

4. Организацию охраны и надежного пропускного режима.

5. Организацию учета, хранения, использования и уничтожения документов и носителей с информацией.

6. Распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.).

7. Организацию явного и скрытого контроля за работой пользователей.

8. Мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Каждая из этих сфер может включать в себя большое количество подуровней, позволяющих более четко рассматривать какие-либо конкретные разделы безопасности. Согласно такому делению на сферы безопасности, например, информационная безопасность будет рассматриваться в каждой из этих сфер следующим образом: на техническом уровне - связанная с повреждением, изменением или утратой, с нарушением работоспособности технических компонент ИС в зависимости от вида воздействия, приведших к такому повреждению или изменению. На программном - повреждение, изменение, утрата или незапланированное политикой безопасности системы распространение информации и т.д.

В общем случае распределенные автоматизированные системы состоят из следующих основных структурно-функциональных элементов [6]:

- рабочих станций - отдельных ЭВМ или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов);
- серверов или Host машин (служб файлов, печати, баз данных и т.п.) не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;
- межсетевых мостов (шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) - элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;
- каналов связи (локальных, телефонных, с узлами коммутации и т.д.).

Рабочие станции [3] являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей.

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей как серверы (Host - машины) и мосты. Первые - как концентраторы больших объемов информации, вторые - как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, наличие возможностей по их надежной защите физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала сети, имеющих непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и преднамеренные воздействия злоумышленников на выделенные серверы и мосты можно считать маловероятными. В то же время, надо ожидать массированной атаки на серверы и мосты с использованием средств удаленного доступа. Здесь злоумышленники прежде всего могут искать возможности повлиять на работу различных подсистем серверов и мос-

тов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам.

Конечно, сказанное выше не означает, что не будет попыток внедрения аппаратных и программных закладок в сами мосты и серверы, открывающих дополнительные широкие возможности по несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных. Возможные при этом угрозы подробно изложены ниже.

Специфика АС, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

Уязвимыми являются буквально все основные структурно-функциональные элементы АС [4]: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи.

Защищать компоненты АС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов путей преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией (в том числе, управляющей согласованным функционированием различных компонентов сети и разграничением ответственности за преобразование и дальнейшую передачу информации).

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики - важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Литература

1. *Домарев В.В.* Защита информации и безопасность компьютерных систем. — К.: ДиаСофт, 2006. — 480 с.

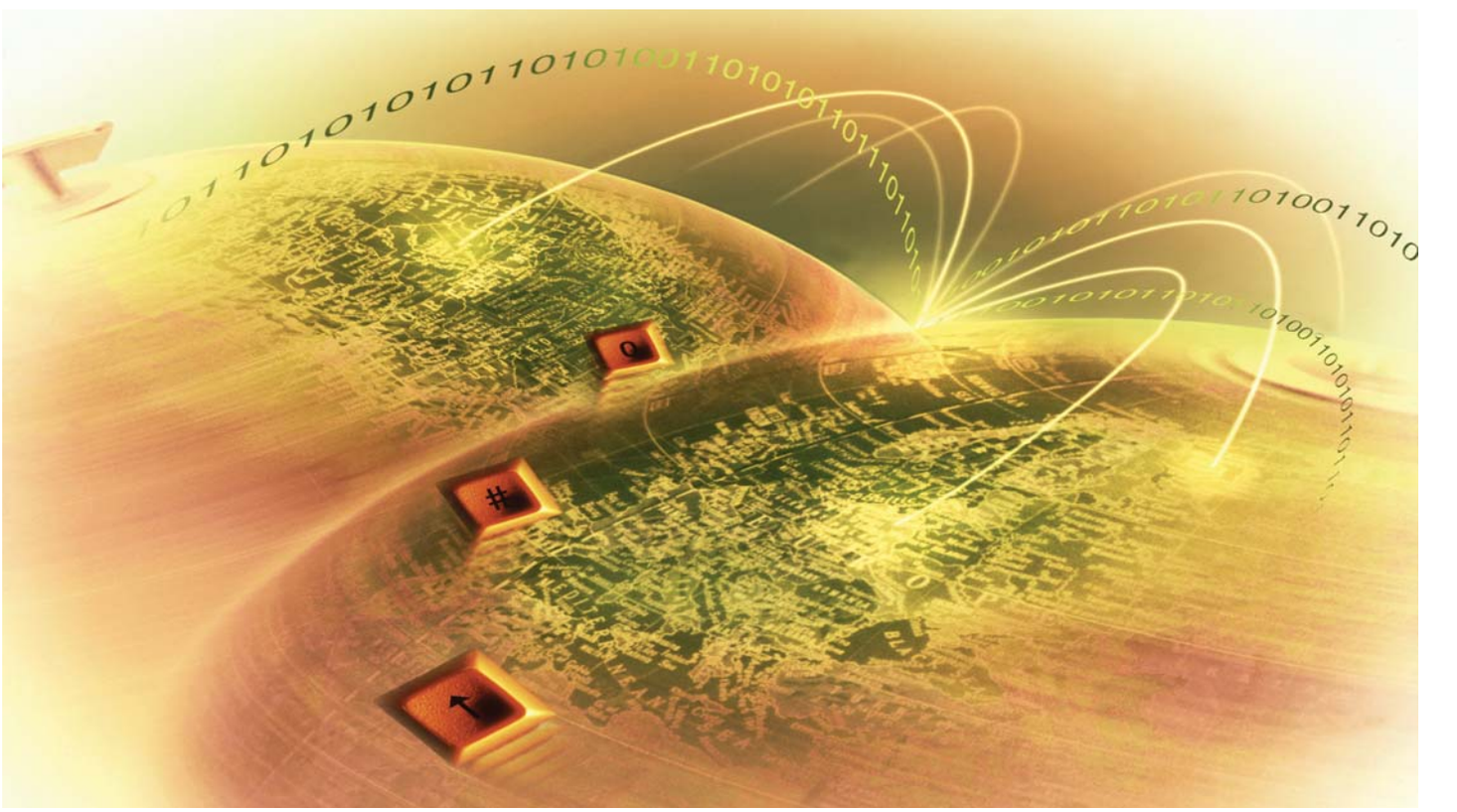
2. *Зайцева И.В., Аверичкин П.А., Романкова М.В.* Современный подход к вопросу об информационной безопасности. Актуальные проблемы информатизации современного общества. Сборник заочного международного научно-практического семинара. - Ставрополь: ООО "Мир данных", 2007, 230 с. — С. 112-115.

3. Информационная безопасность: [сайт]. URL: http://www.itsec.ru.

4. *Торокин А.А.* Инженерно-техническая защита информации: учебное пособие для вузов по специальностям в области информационной безопасности. — М.: Гелиос АРВ, 2005. — 960 с.

5. *Щеглов А. Ю., Тарасюк М.В., Оголюк А.А.* Технология защиты рабочих станций в сетевых архитектурах клиент-сервер. — С.-Петербург: BYTE, 2000. — 320 с.

6. Энциклопедия безопасности: [сайт]. URL: http://www.opasno.net.



Прием навигационного сообщения в аппаратуре потребителя СРНС "Глонасс" в условиях возмущений ионосферы

Как уже было отмечено во многих публикациях в теории приема и обработки сигналов различают когерентную и некогерентную обработку. Оценки псевдо дальностей и псевдо скоростей в приемнике сигналов спутниковой радионавигационной системы могут быть получены как при когерентной, так и при некогерентной обработке сигналов. Выделение же навигационного сообщения возможно лишь в когерентном режиме. Передаваемое в радиосигналах спутниковой радионавигационной системы "Глонасс" навигационное сообщение прежде всего предназначено для проведения потребителями навигационных определений и планирования сеансов навигации. Навигационное сообщение, передаваемое каждым навигационным спутником, содержит оперативную и неоперативную информацию. Оперативная информация содержит: сдвиг шкалы времени навигационного спутника относительно системной шкалы времени; относительное отличие несущей частоты излучаемого радиосигнала от номинального значения; эфемериды навигационного спутника, т.е. координаты и параметры движения спутника на фиксированный момент времени; код метки времени, необходимой для синхронизации процесса извлечения навигационной информации в аппаратуре потребителя. Неоперативная информация содержит альманах системы. В статье рассмотрен вопрос вероятности ошибочного приема навигационного сообщения в аппаратуре потребителя спутниковой радионавигационной системы "Глонасс" в условиях возмущений ионосферы.

Ключевые слова: *спутниковая система, радионавигация, навигационное сообщение, обработка сигналов, когерентный режим.*

Бибарсов М.Р., Грибанов Е.В.,
Военная академия связи имени С.М.Буденного

Reception of the navigation message in equipment of a customer of GLONASS in the conditions of ionosphere perturbations

Bibarsov M.R., Gribanov E.V.,
Military academy of communication of a name of S.M.Budenny

Abstract
As it was already marked in many publications in the theory of reception and signal processing distinguish the coherent and incoherent processing. Estimates pseudo ranges and pseudo speeds in the receiver of signals of satellite radio navigational system can be received both in case of the coherent, and in case of incoherent signal processing. Separation of the navigation message is possible only in the coherent mode. Transferred in wireless signals of satellite radio navigational GLONASS system the navigation message first of all is intended for carrying out by customers of navigation determination and planning of sessions of navigation. The navigation message transferred each navigation satellite, contains operational and not operational information. The operational information contains: shift of a time scale of the navigation satellite of rather system time scale; the relative difference of carrier frequency of an emitted wireless signal from rated value; ephemerises of the navigation satellite, i.e. coordinate and parameters of movement of the satellite on the fixed timepoint; code of the time stamp necessary for synchronization of process of extraction of navigation information in equipment of a customer. Not operational information contains the system almanac. In article the question of probability of erratic reception of the navigation message in equipment of a customer of satellite radio navigational GLONASS system in the conditions of ionosphere perturbations is considered.

Keywords: *satellite system, radio navigation, navigation message, signal processing, the coherent mode.*

Передаваемое в радиосигналах спутниковой радионавигационной системы (СРНС) "Глонасс" навигационное сообщение предназначено для проведения потребителями навигационных определений и планирования сеансов навигации [1]. Навигационное сообщение, передаваемое каждым навигационным спутником (НС), содержит оперативную и неоперативную информацию. Оперативная информация содержит: сдвиг шкалы времени НС относительно системной шкалы времени; относительное отличие несущей частоты излучаемого радиосигнала от номинального значения; эфемериды НС, т.е. координаты и параметры движения спутника на фиксированный момент времени; код метки времени, необходимой для синхронизации процесса извлечения навигационной информации в аппаратуре потребителя. Неоперативная информация содержит альманах системы.

Известно, что в теории приема и обработки сигналов различают когерентную и некогерентную обработку. Оценки псевдо дальностей и псевдо скоростей в приемнике сигналов СРНС могут быть получены как при когерентной, так и при некогерентной обработке сигналов. Выделение же навигационного сообщения возможно лишь в когерентном режиме [1].

Для обеспечения высокой помехоустойчивости и получения высокой точности измерения радионавигационных параметров в СРНС используют сигналы с относительной фазовой манипуляцией (ОФМ) и помехоустойчивое кодирование кодом Хэмминга (88,77) (кодовое расстояние равно 4) [1].

Однако известно, что при естественных (ЕВИ) и искусственных возмущениях ионосферы (ИВИ) возникает рост интегральной электронной концентрации (ЭК) N_T, которая на высотах F слоя имеет неоднородный характер $N_т = \overline{N}_т + \Delta N(\rho)$, где $\overline{N}_т$ и $\Delta N(\rho)$ — среднее значение интегральной ЭК ионосферы и ее флуктуации относительно $\overline{N}_т$ [2, 3].

Увеличение в следствие ЕВИ и ИВИ флуктуаций интегральной ЭК $\Delta N(\rho)$ в слое F, характеризуемых среднеквадратическим отклонением (СКО) $\sigma_{\Delta N_\tau}$, приводит к увеличению СКО флуктуаций фазового фронта волны на выходе ионосферного слоя $\sigma_\varphi \sim \sigma_{\Delta N_\tau}$ и возникновению общих замираний (ОЗ) принимаемых сигналов, т.к. $\gamma^2 \to 0$, где $\gamma^2 \sim 1/\sigma_\varphi$ – коэффициент глубины замираний трансионосферного канала связи (КС) [2,3]. Увеличение σ_φ обуславливает сужение полосы когерентности ионосферы $\Delta F_к \sim 1/\sigma_\varphi$ до $\Delta F_к < 0{,}1$ МГц, что приводит к возникновению частотно-селективных замираний (ЧСЗ) $\Delta F_0 >> \Delta F_к$ [2, 3], т.к. в СРНС используется широкополосный сигнал с шириной спектра $\Delta F_0 = 10$ МГц.

Цель статьи заключается в оценке вероятности ошибочного приема навигационного сообщения в аппаратуре потребителя СРНС «ГЛОНАСС» в условиях возмущений ионосферы.

Вероятность ошибочного приема сигналов ОФМ в каналах с постоянными параметрами и аддитивными гауссовскими шумами при когерентном приеме описывается выражением [4]

$$P_{ош} = \frac{1}{2}\left[1 - F^2\left(\sqrt{2h_0^2}\right)\right], \quad (1)$$

где $F(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}dt$ - интеграл вероятности; h_0^2 – отношение сигнал/шум (ОСШ) на входе приемника.

Для КС с релеевскими замираниями [5]

$$P_{ош} = \frac{1}{2}\int_0^\infty \left[1 - F^2\left(\sqrt{2h^2}\right)\right]\omega\left(h^2\right)dh^2, \quad (2)$$

где $\omega\left(h^2\right) = \frac{2\sqrt{h^2}}{h_0^2}e^{-\frac{h^2}{h_0^2}}$ – плотность распределения вероятности превышения замирающего сигнала.

Интеграл (2) может быть вычислен только приближенными методами [5]. При больших значениях h^2 справедливо соотношение [4]

$$P_{ош} = 1/\left(2 + 3h_0^2\right). \quad (3)$$

Известно, что энергетический выигрыш при использовании когерентного приема при общих замираниях не превышает 3 дБ [6], а т.к. интеграл (2) вычисляется приближенными методами, то для упрощения вычислений можно воспользоваться соотношением, определяющим среднюю вероятность ошибочного приема сигналов ОФМ при некогерентном приеме на выходе демодулятора в виде [6]

$$P_{ош} = \frac{1}{2}\frac{1+\gamma^2}{1+\gamma^2+h_0^2}\exp\left(-\frac{\gamma^2 h_0^2}{1+\gamma^2+h_0^2}\right), \quad (4)$$

где согласно [2, 3]

$$\gamma^2 = 1/\left[\exp\left(\sigma_\varphi^2\right) - 1\right]; \quad (5)$$

$$\sigma_\varphi^2 = \left(80{,}8\pi/c\right)^2\left(\sigma_{\Delta N_\tau}/f_0\right)^2 \quad (6)$$

– дисперсия флуктуаций фазового фронта выходной волны; f_0 – несущая частота; c – скорость света.

Выражение (4) в случае релеевских замираний $\left(\gamma^2 = 0\right)$ сводится к следующему виду [6]

$$P_{ош} = 1/\left(2 + 2h_0^2\right). \quad (7)$$

На рисунке 1 представлены графики зависимости $P_{ош}\left(h_0^2\right)$ при $\gamma^2 = 0$ для когерентного и некогерентного приема, построенные согласно выражений (3), (7)

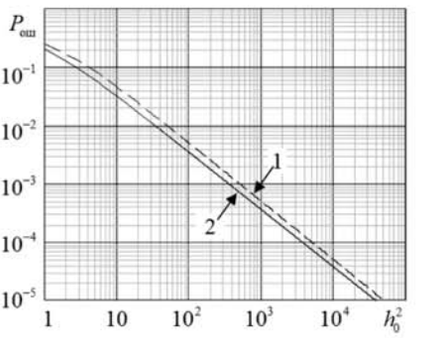


Рис. 1. Зависимость $P_{ош}$ от h_0^2 при $\gamma^2 = 0$ для когерентного (1) и некогерентного (2) приема

Из графиков видно, что выигрыш когерентного приема настолько незначителен, что можно проводить оценку помехоустойчивости когерентного приема согласно выражению (4).

Помехоустойчивое кодирование, реализованное так, как его используют в КС с постоянными параметрами, в каналах с замираниями, хотя и обеспечивает энергетический выигрыш несколько дБ, но ни в коей мере не может компенсировать возникающие потери помехоустойчивости [7]. В связи с этим, для оценки вероятности ошибочного приема навигационного сообщения СРНС «ГЛОНАСС» в КС с ОЗ справедливо использовать соотношение (4).

При модели КС с ЧСЗ, когда спектральные составляющие $\Omega = 2\pi(f - f_0)$ сигнала в пределах полосы его спектра $\Delta\Omega_0 = 2\pi\Delta F_0$ замирают по релеевскому закону, но некоррелированно, ОСШ на входе приемника h_0^2 уменьшится в $\eta_ч$ раз, где $\eta_ч \le 1$ – коэффициент энергетических потерь при обработке (в согласованном фильтре или корреляторе) сигнала, подверженного ЧСЗ [2, 3]. Величина данного коэффициента определяется как

$$\eta_ч = \operatorname{erf}\left[\pi\left(\Delta F_к/\Delta F_0\right)\right]\left[1 + \left(2\pi^2\right)^{-1}\left(\Delta F_0/\Delta F_к\right)^2\right] - \pi^{3/2}\left(\Delta F_0/\Delta F_к\right)\left\{2 - \exp\left[-\pi^2\left(\Delta F_к/\Delta F_0\right)^2\right]\right\}, \quad (8)$$

где

$$\Delta F_к = 2f_0/\left[\sigma_\varphi\left(2 + d_1^2\right)^{1/2}\right]; \quad (9)$$

$d_1^2 \geq 1$ – коэффициент, характеризующий нарастание дифракционных эффектов во фронте волны по мере ее распространения, определяемый как

$$d_1^2 = \left(h_э^2 - 3h_э h_1 + 3h_1^2\right)c^2 \Big/ 192\pi^2 f_0^2 l_s^4, \qquad (10)$$

$h_1 = 5 \cdot 10^5$ м – расстояние от нижней границы ионосферного слоя до точки приема; $h_э = 2{,}55 \cdot 10^5$ м – эквивалентная толщина слоя F ионосферы с неизменным по высоте значением ЭК; $l_s = 200$ м – характерный размер мелкомасштабных неоднородностей.

С учетом ЧСЗ выражение (4) примет вид

$$P_{ош} = \frac{1}{2}\frac{1+\gamma^2}{1+\gamma^2+h_0^2\eta_ч}\exp\left(-\frac{\gamma^2 h_0^2 \eta_ч}{1+\gamma^2+h_0^2\eta_ч}\right). \qquad (11)$$

В таблице 1 представлены параметры ионосферы [2, 3] при различном ее состоянии, для которых на рисунке 2 представлены графики зависимости $P_{ош}\left(h_0^2\right)$, построенные согласно (11).

Таблица 1

Параметры ионосферы в зависимости от ее состояния

Состояние ионосферы	$\overline{N}_m$, эл/м^3	$\overline{N}_т$, эл/м^2	$\sigma_{\Delta N_т}$, эл/м^2
Невозмущенная ионосфера (НИ)	10^{12}	$2{,}55 \cdot 10^{17}$	10^{13}
ЕВИ	10^{13}	$2{,}55 \cdot 10^{18}$	10^{15}
ИВИ	10^{14}	$2{,}55 \cdot 10^{19}$	10^{17}

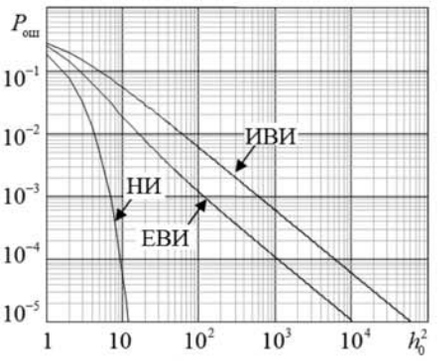


Рис. 2. Зависимость $P_{ош}$ от h_0^2 при различном состоянии ионосферы

Из графиков видно, что в условиях НИ вероятность ошибочного приема навигационного сообщения $P_{ош} = 10^{-5}$ обеспечивается при ОСШ на входе приемника $h_0^2 = 11\,(10\text{ дБ})$, в условиях ЕВИ при ОСШ $h_0^2 = 10^4\,(40\text{ дБ})$, а в условиях ИВИ при ОСШ $h_0^2 = 6 \cdot 10^4\,(48\text{ дБ})$.

Известно, что повышение помехоустойчивости возможно применением пространственно-разнесенного приема на несколько антенн (n), расположенных на расстояниях превышающих интервал пространственной корреляции замираний. При этом в устройстве обработки сигналов используют различные алгоритмы, например когерентного сложения с весами, выигрыш от которого больше, чем при квадратичном сложение всего на 1-2 дБ при достаточно сложной его реализации [7].

Вероятность ошибки в схеме квадратичного сложения определяется согласно выражению [8]

$$P_{ош} = \sum_{k=0}^{n-1} C_{n+k-1}^k P_{ош1}^n \left(1 - P_{ош1}\right)^k, \qquad (12)$$

где $P_{ош1}$ – вероятность ошибки при одиночном некогерентном приеме для того же значения h_0^2.

Эта же формула справедлива и для оптимального когерентного разнесенного приема, если под $P_{ош1}$ понимать вероятность ошибки при оптимальном когерентном одиночном приеме [8].

На рисунке 3 представлены графики зависимости $P_{ош}\left(h_0^2\right)$ в условиях ИВИ, построенные согласно (11) и (12) для пространственно-разнесенного приема на $n = 2$, $n = 3$ и $n = 4$ антенны.

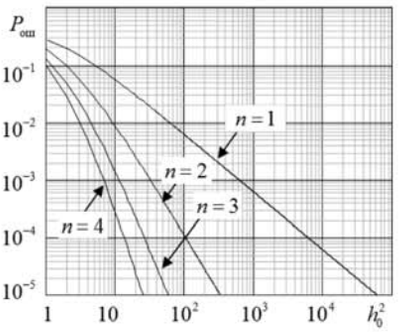


Рис. 3. Зависимость $P_{ош}$ от h_0^2 в условиях ИВИ при пространственно-разнесенном приеме на n антенн

Следует отметить, что результаты расчета согласно выражению (11) совпадают с результатами расчета согласно (12) при $n = 1$.

Таким образом, при реализуемом ОСШ на входе приемника СРНС «ГЛОНАСС» $h_0^2 = 20$ дБ, в условиях ИВИ вероятность ошибочного приема навигационного сообщения в аппаратуре потребителя СРНС «ГЛОНАСС» составит $P_{ош} = 6 \cdot 10^{-3}$. При пространственно-разнесенном приеме на $n = 2$ антенны вероятность ошибочного приема навигационного сообщения уменьшится до $P_{ош} = 10^{-4}$, при $n = 3$ и $n = 4$ до $P_{ош} << 10^{-5}$.

Следовательно, существенное влияние на вероятность ошибочного приема навигационного сообщения $(P_{ош})$ СРНС оказывает фактор рассеяния радиоволн в неоднородностях ионосферы, проявляющийся в виде замираний принимаемых сигналов, которые могут носить общий (райсовский, релеевский) или частотно-селективный характер в зависимости от частотных параметров $(f_0, \Delta F_0)$ передаваемых сигналов и степени возмущения неоднородной ионосферы.

Следует отметить, что в условиях НИ (когда $\sigma_{\Delta N_т} = 10^{13}$ эл/м^2) $P_{ош} \le 10^{-5}$ достигается за счет выбора частотных параметров $f_0 = 1{,}6$ ГГц и $\Delta F_0 = 10$ МГц, при которых фактор рассеяния радиоволн на неоднородностях ионосферы не проявляется и замирания принимаемых сигналов отсутствуют.

Однако в условиях ИВИ, когда ($\sigma_{\Delta N_т} = 10^{17}$ эл/м^2) передача сигналов с указанными частотными параметрами ($f_0 = 1{,}6$ ГГц, $\Delta F_0 = 10$ МГц) может сопровождаться существенным увеличением вероятности ошибочного приема навигационного сообщения ($P_{ош}$).

Литература

1. ГЛОНАСС. Принципы построения и функционирования / Под ред. А.И.Перова, В.Н. Харисова. Изд. 4-е, перераб. и доп. – М.: Радиотехника, 2010. – 800 с.
2. *Маслов О.Н., Пашинцев В.П.* Модели трансионосферных радиоканалов и помехоустойчивость систем космической связи / Приложение к журналу "Инфокоммуникационные технологии". Выпуск 4. – Самара: ПГАТИ, 2006. – 357 с.
3. *Пашинцев В.П., Солчатов М.Э., Гахов Р.П.* Влияние ионосферы на характеристики космических систем передачи информации: Монография. – М.: Физматлит, 2006. – 184 с.
4. *Игнатов В.В., Килимник Ю.П., Никольский И.Н., Пивоваров В.Ф., Прохоров В.К., Репин Г.А., Скрипник Н.П., Шаров А.Н.* Военные системы радиосвязи. Ч.1. / Под ред. В.В. Игнатова. – Л.: ВАС, 1989. – С. 1-386.
5. *Буга Н.Н.* Основы теории связи и передачи данных. Ч.2. Учебник для слушателей военных академий и высших командно-инженерных училищ. – Л енинград, 1970. – 707 с.
6. *Финк Л.М.* Теория передачи дискретных сообщений. Изд. 2-е, переработанное, дополненное. Издательство «Советское радио», 1970. – С.728.
7. *Волков Л.Н., Немировский М.С., Шинаков Ю.С.* Системы цифровой радиосвязи: базовые методы и характеристики: Учеб. пособие. – М.: Эко-Трендз, 2005. – 392 с.
8. *Бураченко Д.Л., Заварин Г.Д., Клюев Н.И., Колесников А.А., Кондратьев С.Л., Коржик В.И., Финк Л.М.* Общая теория связи. – ВАС, 1970. – С. 1-412.

К вопросу решения антагонистических задач при комплексном противодействии сторон

Проведенные анализы алгоритмов функционирования системы воздействия показали, что перед активным воздействием осуществляется фаза наблюдения за элементами системы. После чего выполняется фаза информационного воздействия и (или) силового (контактного) воздействия. Следовательно, можно сформулировать следующий последовательно-параллельный алгоритм комплексного воздействия: детальное и глубокое техническое наблюдение за элементами системы защиты с установлением их местоположения, важности, связности (вскрытие топологии и функциональных взаимосвязей); затем принятие решения по информационному и (или) силовому воздействию. Таким образом необходимо рассмотреть метод решения антагонистических задач при комплексном противодействии сторон, который и рассмотрен в статье.

Ключевые слова: *система защиты, модель системы, наблюдение, информационное воздействие, силовое воздействие.*

Якушенко С.А., Прасько Г.А., Дворовой М.О., Веркин С.С.,
Военная академия связи имени С.М.Буденного

Solution of antagonistic tasks in case of complex counteraction of the sides

Yakushenko S.A., Prasko G.A., Dvorovoy M.O., Verkin S.S.,
Military academy of communication of a name of S.M.Budenny

Abstract
The carried-out analyses of algorithms of functioning of system of influence showed that before the active influence the phase of observation over system elements is carried out. Then the phase of information influence and (or) force (contact) influence is executed. Therefore, it is possible to formulate the following serial-to-parallel algorithm of complex influence: detail and deep technical observation over elements of system of protection with establishment of their location, importance, connectivity (opening of topology and the functional correlations); then decision-making on information and (or) force influence. Thus it is necessary to consider a method of the solution of antagonistic tasks in case of complex counteraction of the sides which is considered in article.

Keywords: *protection system, system model, observation, information influence, force influence.*

Анализ функциональных моделей антагонистических систем, позволяет выявить логику их действия в конфликтной ситуации:

1. Наблюдение. Данный вид пассивного воздействия важен на первоначальном этапе формирования системы защиты (система А), так как в этот период она в априори неизвестна системе воздействия (система Б).

2. Информационное воздействие (ИВ) и радиоэлектронное воздействие.

3. Силовое (контактное) воздействие (СВ). Осуществляется на основе априорных сведений о системе защиты.

Так как ресурс средств воздействия ограничен, то система воздействия будет стремиться так, распределить свои средства нападения, чтобы нанести максимальный ущерб системе защиты. В результате оптимального распределения ресурса воздействия (средств ИВ и СВ) по объектам системы защиты, сформируется стратегия комплексного воздействия, наносящая максимальный ущерб

$$\max_j \hat{h}_{ij} = \max_{\{R\}} P_{\text{н}rj} \max_{\{N\}} P_{\text{ив}nj} \max_{\{V\}} P_{\text{св}vj} \qquad (1)$$

Очевидно, что количество оптимальных стратегий будет определяться выделенным ресурсом ИВ и СВ со стороны воздействия и ресурсом для построения системы и мер защиты (противодействием) со стороны системы защиты. Причем защита может иметь как пассивный, так и (или) активный характер, в зависимости от выбранной стратегии защиты.

Анализ алгоритмов функционирования системы воздействия показывает, что перед активным воздействием осуществляется фаза наблюдения за элементами системы. После чего выполняется фаза ИВ и (или) СВ. Следовательно, можно сформулировать следующий последовательно-параллельный алгоритм комплексного воздействия: детальное и глубокое техническое наблюдение за элементами системы стороны А с установлением их местоположения, важности, связности (вскрытие топологии и функциональных взаимосвязей); затем принятие решения по ИВ и (или) СВ (рис. 1).

Критерием системы воздействия по вскрытию элементов системы защиты является максимум функции (1).

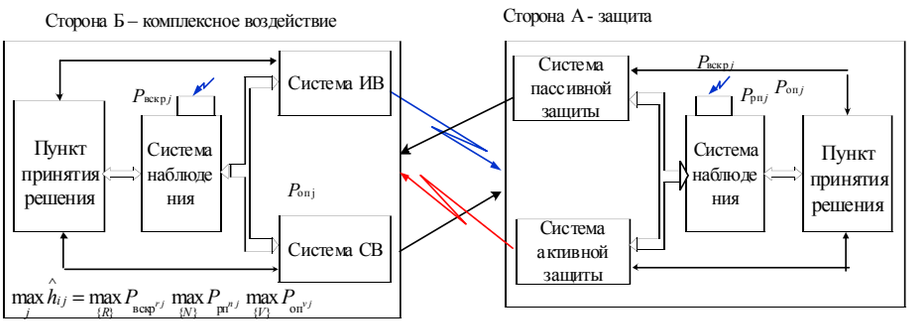


Рис. 1. Модель комплексного воздействия на систему

Тогда задача выбора оптимальной стратегии наблюдения будет заключаться в нахождении матрицы назначения элементов множества $\{R\}$ по элементам множества $\{S\}(R=||\rho_{ri}||_{RS})$, доставляющей максимальное значение функции

$$p_{н}(S)=F(R^{o})=\max_{\rho,\{x,y,h\}}\sum_{i=1}^{S}A_i\left\{1-\prod_{j=1}^{S}\left[1-\alpha_{ji}\left(1-\prod_{r=1}^{R}\left(1-p_{н\,ri}(x,y,h)\right)^{\rho_{ri}}\right)\right]\right\}. \quad (2)$$

При следующих ограничениях и условиях:

$$\sum_{j=1}^{S}\rho_{ri}=1;\ 0\le p_{н\,ri}(x,y,h)\le 1;\ 0<A_i<1;$$
$$0\le\alpha_{ji}\le 1;\ \alpha_{ii}=1;\ r=\overline{1,R};\ i,j=\overline{1,S}, \quad (3)$$

Индекс назначение элементов означает, что если ρ_{ri}=1, то *r*-е средство назначено для наблюдения за *i*-м объектом, а если ρ_{ri}=0, то не назначено.

Решение данной задачи осуществляется методом двух функций. Результатом решения является оптимальная матрица назначения средств наблюдения по объектам $R=||\rho_{ri}||_{RS}$. При этом значение целевой функции характеризует математическое ожидание количества вскрытых объектов.

Критерием нанесения ущерба системой активного воздействия (ИВ и СВ) элементам системы защиты является максимизация функций (2) и (3). Тогда задача выбора оптимальной стратегии активного воздействия на систему защиты будет заключаться в нахождении матрицы назначения средств ИВ и СВ по элементам системы ($\Omega=\|\omega_{bi}\|_{BS}$), доставляющая максимум целевой функции

$$p_{возд}(S)=F(\Omega_0)=\max_{\omega,\{x,y,h\}}\times \quad (4)$$
$$\times\sum_{i=1}^{S}A_i\left\{1-\prod_{j=1}^{S}\left[1-\alpha_{ji}\left(1-\prod_{v=1}^{B}\left(1-p_{ив\,bi}\vee p_{св\,bi}(x,y,h)\right)^{\omega_{bi}}\right)\right]\right\},$$

при следующих ограничениях:

$$\sum_{i=1}^{S}\omega_{bi}=1;\ 0<p_{ив\,bi}(x,y,h)\le 1;\ 0<A_i\le 1;\ 0\le\alpha_{ji}\le 1;$$
$$b=\overline{1,B};\ i,j=\overline{1,S};\ \{B\}=\{N\}\cap\{V\}, \quad (5)$$

где $\{B\}=\{N\}\cap\{V\}$ означает множество средств, принадлежащих *R* или *V*.

Индекс назначение элементов означает, что если ω_{b_i}=1, то *b*-е средство воздействия (РП $\wedge$ ОП, где $\vee$ – знак *или*) назначено для нанесения ущерба *i*-му объекту, а если ω_{b_i} = 0, то не назначено.

Решение данной задачи осуществляется также методом двух функций. Результатом решения является оптимальная матрица назначения средств ИВ по объектам системы защиты $\Omega^{o}=\|\omega_{bi}\|_{BS}$. При этом значение целевой функции характеризует математическое ожидание объектов, по которым назначены средства нападения с учетом эффективности их воздействия (нанесения ущерба).

Вскрытие элементов системы защиты, как было отмечено выше, осуществляется на основе формирования оптимальной стратегии наблюдения (2), по результатам которой ресурс воздействия (ИВ и СВ) распределяется по элементам системы защиты наилучшим образом. Тогда физическая постановка задачи можно сформулировать следующим образом. При построении топологии системы защиты необходимо так расположить элементы системы, чтобы вероятность их вскрытия была минимальной, варьируя защитным ресурсом подсистемы (энергетическим, частотным, сигнальным и пространственным) при выполнении остальных требований. Предположим, что элементы системы защиты создают некое поле на территории размером *a* x *b* для обслуживания различных по приоритету объектов. Поэтому каждый объект характеризуется вектором весов $A=\{A_i\}$, $i=\overline{1,S'}$, определяющих их важность, причем $S'\in S$. Элементы системы взаимосвязаны обменом информации и территориями (зонами) обслуживания α_{ij}. Возможности наблюдения заданы матрицей $||\rho_{ni}||_{RS'}$ (*R* – назначенные средства наблюдения за элементами системы защиты в результате решения задачи выбора оптимальной стратегии), а возможность силового и информационного воздействия на элементы системы заданы матрицами $||\rho_{свni}||_{NS'}$, и $||\rho_{ивvi}||_{VS'}$.

Необходимо определить местоположение элементов системы защиты и их количество, т.е. синтезировать ее топологию, чтобы обеспечить максимальную ее устойчивость функционирования в смысле информационной и силовой защищенности при выполнении остальных требований предъявляемых к системе.

Содержательная постановка задачи. Требуется определить матрицу назначения координат элементов системы (*x,y,h*) доставляющую максимальное значение целевой функции

$$P_{защ}\left(S\left(x^{o},y^{o},h^{o}\right)\right)=\max_{\substack{\rho,\omega,\varepsilon\\{x,y,h}\}}\sum_{i=1}^{S}A_i\times \quad (6)$$
$$\times\left\{1-\prod_{r=1}^{R}\left[1-\alpha_{ji}\left(p_{н\,ri}(x,y,h)\right)^{\rho_{ri}}\left(1-\prod_{b=1}^{B}\left(p_{возд\,bi}(x,y,h)^{\omega_{bi}}\left(1-\prod_{m=1}^{M}q_{mr(b)i}^{\varepsilon_{mr(b)i}}\right)\right)\right)\right]\right\}$$

при следующих ограничениях и условиях:

$$0<p_{н\,ri}(x,y,h)<1;\ 0<p_{возд\,bi}(x,y,h)<1;\ 0<q_{mr(b)i}<1;\ 0<A_i<1;$$
$$\sum_{j=1}^{S}\rho_{ri}=1;\ \sum_{j=1}^{S}\omega_{bi}=1;\ \sum_{j=1}^{S}\varepsilon_{mr(b)i}=1;\ i,j=\overline{1,S'};$$
$$m=\overline{1,M};\ r=\overline{1,R};\ b=\overline{1,B};$$
$$M<S';\ R<S';\ B<S',\ \sigma\le\sigma_{н};\ p_{д}\ge p_{дн}, \quad (7)$$

где (*x,y,h*)–возможные координаты точек размещения элементов системы защиты; (*x,y,h*)–оптимальные координаты элементов; $p_{н\,ri}(x,y,h)$–вероятность вскрытия *i*-го элемента с координатами (*x, y, h*) *r*-м средством наблюдения системы воздействия, т.е. при ρ_{ri}=1; $p_{возд\,bi}(x,y,h)$–вероятность нанесения ущерба *i*-му элементу с координатами (*x, y, h*) *b*-м средством силового (или информационного) воздействия ($p_{св\,bi}\vee p_{ив\,bi}$) при условии его назначения на этот элемент, т.е. при ω_{bi}=1; $q_{mr(b)i}$–вероятность защиты *i*-го элемента *m*-ресурсом защиты при использовании *r*-го средства наблюдения и *b*-го средства воздействия и при условии назначения данного ресурса защиты, т.е. при $\varepsilon_{mr(b)i}$=1; $A=\{A_i\}$, $i=\overline{1,S'}$–важность элемента системы; σ - точность определения координат; $p_{д}$–доступность абонентов к системе.

Метод и алгоритм решения задачи. Задача поиска координат для развертывания системы носит оптимизационный характер и может быть решена одним из методов оптимизации. Так как система действий поиска строго предопределяется сложившейся ситуацией, определяемой группировкой средств

воздействия и ресурсом средств, для развертывания элементов системы, то алгоритм поиска носит регулярный (детерминированный) характер. Это значит, что в одинаковых ситуациях система действий будет также одинакова в противоположность случайным процессам (алгоритмам), которые допускают неодинаковую систему действий в тождественных ситуациях.

Методами решения таких задач являются: метод сканирования; метод поочередного изменения параметров (Гаусса-Зейделя); метод «тяжелого шарика»; градиентный метод; метод наискорейшего спуска и метод сканирования.

Анализ целевой функции показывает, что она относится к классу аддитивных целочисленных функций с ограничениями смешанного типа. Варьируемыми параметрами целевой функции являются вероятностные характеристики вскрытия элементов средствами наблюдения (пассивное воздействие), силового и информационного воздействия по элементам системы защиты (активное воздействие), а также пространственные, частотные, энергетические, сигнальные и другие ресурсы защиты системы. Значение вероятностей, в свою очередь, зависят от энергетических соотношений как на измерительных радиолиниях, так и на трассе наблюдения для заданных координат (x,y,h). Кроме того, значение целевой функции определяется весом элементов системы. Тогда в результате поиска их оптимального местоположения – изменения координат (x,y,h), значение целевой функции будет изменяться то в большую, то в меньшую сторону в зависимости от дальности наблюдения и воздействия, защитных ресурсов и т.п. Следовательно, целевая функция относится к классу нелинейных, выпуклых аддитивных функций с условной оптимизацией целочисленного типа.

В этом случае приемлемым методом ее решения является метод сканирования, так как во-первых целевая функция имеет сложную зависимость от изменяемых параметров (пространственных, энергетических, весовых), а во-вторых метод сканирования не накладывает никаких ограничений на вид целевой функции. Суть метода заключается в определении и сравнении значений целевой функции во всех узлах сетки как показано на рис. 2.

Расчет обычно начинается с левого верхнего узла и слева направо, снизу вверх, в зависимости от того, какая переменная меняется во внутреннем цикле ($x_i+\Delta x$; $y_i+\Delta y$) затем осуществляется сканирование по вертикали $h_i+\Delta h$ в пределах допустимых значений. Точность решения задачи методом сканирования зависит от величины шага сканирования $(\Delta x,\Delta y,\Delta h)$. Причем уменьшение шага приводит к квадратичному увеличению числа расчетных процедур.

В результате поиска определяются оптимального местоположения элементов системы с точки зрения защиты от комплексного воздействия. Поиск продолжается до тех пор, пока существует область поиска или выделенный ресурс защиты элементов системы при выполнении остальных требований. Для этого цикл поиска в заданной области повторяется, причем район, «обслуженный» элемент из области поиска исключается. В результате второго цикла поиска определяется местоположение второго по оптимальности элемента и т. д.

В конце поиска будет найдено минимальное количество элементов, задействованных в системе. Полученная топология будет иметь максимальную устойчивость функционирования (информационную и силовую защищенность).

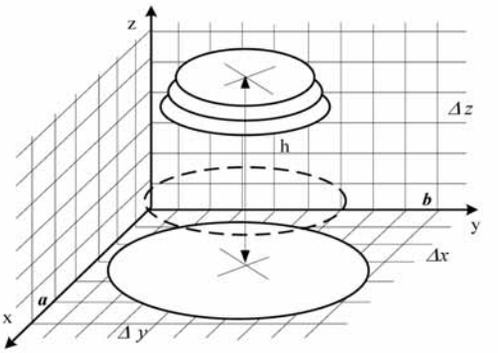


Рис. 2. Пояснение метода «сканирования»

Алгоритм реализации метода сканирования для данного случая приведен на рис. 3.

Достоинством данного метода является простота и возможность точного получения оптимального решения. Однако увеличение размерности задачи (уменьшение шага сканирования) и количества элементов приводит к значительному росту объема вычислений. Тем не менее, такой подход является предпочтительнее в случае выбора оптимальной топологии системы. Точность метода целиком и полностью определяется корректностью выбора исходных данных, полнотой множества вариантов структуры системы и шагом сканирования.

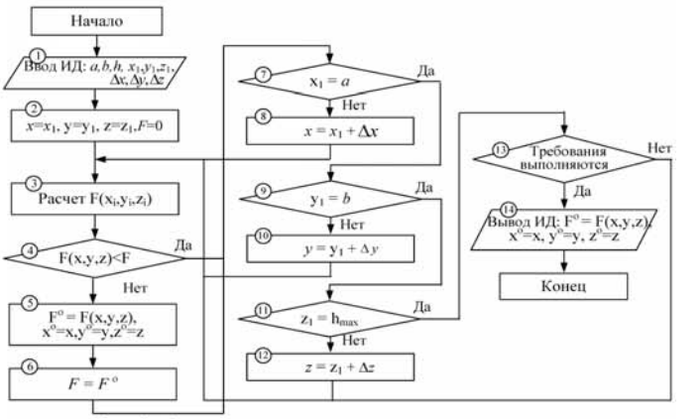


Рис. 3. Алгоритм реализации метода сканирования

Литература

1. *Бронштейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся ВТУЗов. – М.: Наука, Гл. ред. физ-мат. лит., 1986. – 544 с.

2. *Роджерс К.* Укладки и покрытия. – М.: Мир, 1968. – 132 с.

3. *Берзин Е.А.* Оптимальное распределение ресурсов и теория игр. – М.: Сов. радио, 1983. – 215 с.

5. *Снежко В.К. Прасько Г.А.* О рабочих зонах позиционирования в сетях сухопутной подвижной радиосвязи // Технологии и средства связи, 2008. №4.

6. *Снежко В.К., Якушенко С.А.* Интегрированные системы навигации, связи и управления сухопутных подвижных объектов: Учеб. пособие для ВУЗов связи. СПб.:ВАС, 2008. – 308 с.

7. *Стоян Ю.Г., Яковлев С.В.* Математические модели и оптимизационные методы геометрического проектирования. – Киев: Наук. думка, 1986. – 268 с.

Алгоритм формирования остатков в расширенных полях

В настоящее время существующие алгоритмы, используемые в теории кодирования, криптографических приложениях, устройствах цифровой обработки сигналов и устройствах обмена цифровой информацией используют процедуры вычисления остатков в конечных полях. Вычисление остатков в расширенных полях GF(pn) в основном сводится к процедуре последовательного деления, что в случае больших массивов данных приводит к значительным временным затратам. Кроме того, известные алгоритмы формирования остатков в расширенных полях GF(pn) реализованы для частных случаев модуля p и расширения поля степени n и не позволяют выполнять вычисления для произвольных значений p и n. В связи с этим для большинства приложений, использующих теорию конечных полей, являются актуальными вопросами построения алгоритмов формирования остатков для расширенных полей с произвольными значениями p и n. Целью статьи является разработка алгоритма формирования остатков в расширенных полях GF(pn) с произвольными значениями p и n.

Ключевые слова: *алгоритм, расширенные поля, теория кодирования, криптография, цифровая обработка сигналов.*

Петренко В.И., Кузьминов Ю.В.,
Ставропольский государственный университет

Residuals formation algorithm in expanded fields

Petrenko V. I., Kuzminov Yu.V.,
Stavropol state university

Abstract

Now the existing algorithms used in the coding theory, cryptography applications, devices of digital signal processing and devices of an exchange of digital information use procedures of computation of residuals in finite fields. Computation of residuals in the expanded GF (pn) fields is generally reduced to procedure of sequential division that in case of data bulks leads to the considerable time expenditure. Besides, known algorithms of formation of residuals in the expanded GF (pn) fields are implemented for special cases of the module p and extension of a field of a level of n and don't allow to execute computation for arbitrary values of p and n. In this regard for the majority of the applications using the theory of finite fields, are topical issues of creation of algorithms of formation of residuals for expanded fields with arbitrary values of p and n. The purpose of article is development of algorithm of formation of residuals in the expanded GF (pn) fields with arbitrary values of p and n.

Keywords: *algorithm, expanded fields, coding theory, cryptography, digital signal processing.*

Большинство современных алгоритмов, используемых в теории кодирования, криптографических приложениях, устройствах цифровой обработки сигналов и устройствах обмена цифровой информацией используют процедуры вычисления остатков в конечных полях [1]. Однако, если для простых полей Галуа $GF(p)$ существует ряд достаточно эффективных способов формирования остатков, то вычисление остатков в расширенных полях $GF(p^n)$ в основном сводится к процедуре последовательного деления, что в случае больших массивов данных приводит к значительным временным затратам. Кроме того, известные алгоритмы формирования остатков в расширенных полях $GF(p^n)$ реализованы для частных случаев модуля p и расширения поля степени n и не позволяют выполнять вычисления для произвольных значений p и n. В связи с этим для большинства приложений, использующих теорию конечных полей, являются актуальными вопросами построения алгоритмов формирования остатков для расширенных полей с произвольными значениями p и n.

Целью нашего исследования является разработка алгоритма формирования остатков в расширенных полях $GF(p^n)$ с произвольными значениями p и n.

Для вывода обобщенного аналитического выражения процесса формирования остатка введем следующие обозначения.

Пусть $A(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ и $F(x) = b_k x^k + b_{k-1}x^{k-1} + ... + b_1 x + b_0$ — полиномы над полем $GF(p^n)$, причем $k \le n$. Наибольший практический интерес представляет случай, когда используемый для получения остатка от полинома $A(x)$ по двойному модулю $(F(x), p)$ полином $F(x)$ является неприводимым над полем $GF(p^n)$ и нормированным, то есть приведенным к виду $F(x) = x^k + b_{k-1}x^{k-1} + ... + b_1 x + b_0$.

Процесс формирования остатка начинается с вычисления частичного остатка младшей степени полинома $A(x)$ по двойному модулю $(F(x), p)$ с последующим увеличением степени на один разряд. Очевидно, что при всех значениях степени полинома $F(x)$, меньших k, частичным остатком будет являться значение самого делимого.

Рассмотрим процесс формирования частичных остатков при достижении степенью полинома $A(x)$ значения k.

Пусть c_i — коэффициенты при степенях частичного остатка, полученного по завершении k-й операции. В общем виде данный частичный остаток $R_ч(x)$ можно представить выражением:

$$R_ч(x) = c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + ... + c_1 x + c_0 \qquad (1)$$

Согласно вышеприведенному алгоритму, степень частичного остатка необходимо увеличить на один разряд, что эквивалентно умножению выражения на x:

$$R^*_ч(x) = (c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + ... + c_1 x + c_0)x = \\ = c_{k-1}x^k + c_{k-2}x^{k-1} + ... + c_1 x^2 + c_0 x. \qquad (2)$$

Полученное в (2) выражение служит делимым для вычисления частичного остатка от (k+1)-й степени полинома $A(x)$. Для осуществления указанной операции полином $F(x)$ необходимо умножить на коэффициент при k-й степени частичного остатка:

$$F^*(x) = c_{k-1}F(x) = c_{k-1}(x^k + b_{k-1}x^{k-1} + ... + b_1x + b_0) = \\ = c_{k-1}x^k + c_{k-1}b_{k-1}x^{k-1} + ... + c_{k-1}b_1x + c_{k-1}b_0. \quad (3)$$

Далее выражение (3) необходимо вычесть из делимого (2):

$$R_v^*(x) - F^*(x) = (c_{k-1}x^k + c_{k-2}x^{k-1} + ... + c_1x^2 + c_0x) - (c_{k-1}x^k + c_{k-1}b_{k-1}x^{k-1} + ... + c_{k-1}b_0) = \\ = c_{k-1}x^k + c_{k-2}x^{k-1} + ... + c_1x^2 + c_0x - c_{k-1}x^k - c_{k-1}b_{k-1}x^{k-1} - ... - c_{k-1}b_0 = \\ = x^{k-1}(c_{k-2} - c_{k-1}b_{k-1}) + x^{k-2}(c_{k-3} - c_{k-1}b_{k-2}) + ... + x(c_0 - c_{k-1}b_1) + (-c_{k-1}b_0). \quad (4)$$

Значения выражений в скобках по сути являются коэффициентами c_i при степенях частичного остатка $R_v(x)$ в выражении (1).

Вышеуказанные операции вычисления частичных остатков производятся для каждой степени полинома $A(x)$, после чего каждый полученный частичный остаток от степени полинома $A(x)$ умножается на коэффициент при данной степени. Результаты умножения суммируются по модулю p, а результат суммирования представляет собой остаток от полинома $A(x)$ по двойному модулю ($F(x)$, p).

В общем виде остаток $R(x)$ от полинома $A(x)$ над полем $GF(p^n)$ по двойному модулю ($F(x)$, p) можно записать в виде

$$R(x) = \sum_{i=0}^{n} a_i R_{vi}(x) \quad (5)$$

Таким образом, выражение (4) представляет собой обобщенное правило формирования частичных остатков от произвольного полинома над полем $GF(p^n)$ по двойному модулю.

Алгоритм формирования остатков в расширенных полях, основанный на вычислении частичных остатков от степеней полинома с последующим их суммированием в соответствии со значением коэффициента при данной степени может быть описан следующими шагами:

1. Вычисляется частичный остаток от младшей степени полинома.
2. Полученный частичный остаток умножается на коэффициент при этой же степени полинома.
3. Результат умножения накапливается в суммирующем устройстве.
4. Степень сформированного частичного остатка увеличивается на один разряд.
5. От полученного выражения также вычисляется частичный остаток, с которым производятся операции согласно пунктов 2-4.
6. По завершении n-й операции на выходе суммирующего устройства формируется остаток от исходного полинома над полем $GF(p^n)$ по двойному модулю.

Устройство, реализующее предложенный алгоритм представлено на рисунках 1-3 [2]. На рисунке 1 представлена схема устройства формирования остатка по двойному модулю, на рисунке 2 – схема блока формирования частичных остатков, на рисунке 3 – схема блока формирования коэффициентов.

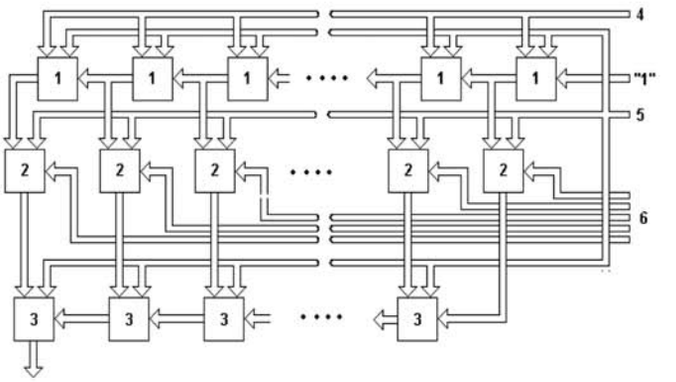


Рис. 1. Устройство формирования остатка по двойному модулю:
1 – блок формирования частичных остатков;
2 – умножитель по модулю, 3-сумматор по модулю

Устройство формирования остатка по двойному модулю состоит из (n+1) последовательно соединенных блоков 1 формирования частичных остатков, (n+1) умножителей 2 по модулю и n сумматоров 3 по модулю (см. рис. 1).

Первый вход первого блока 1 формирования частичных остатков служит для записи кода «1», являющегося кодом начала операции, на первый вход каждого из последующих блоков 1 формирования частичных остатков подаются выходы разрядов предыдущего блока 1 формирования частичных остатков со сдвигом на один разряд в сторону старшего. Второй вход каждого блока 1 формирования частичных остатков служит для записи кода модуля p, поступающего со входа 5 устройства. На третий вход каждого блока 1 формирования частичных остатков подаются коэффициенты полинома модуля. На третий вход каждого умножителя 2 по модулю подается код модуля p со входа 5 устройства. На третий вход каждого сумматора 3 по модулю подается код модуля p со входа 5 устройства. Выход n-го сумматора является выходом устройства.

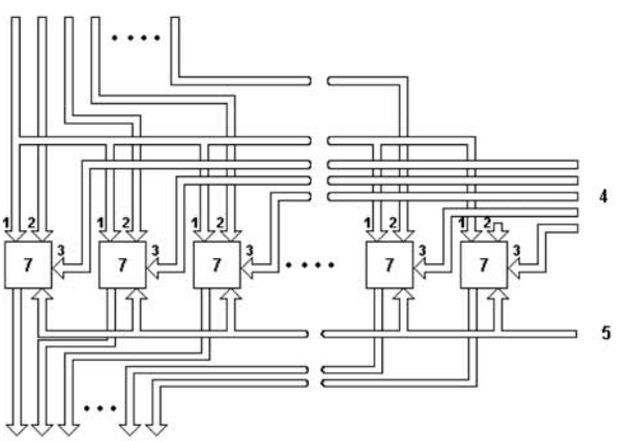


Рис. 2. Блок формирования частичных остатков

Блок 1 формирования частичных остатков (см. рис. 2) содержит k блоков 7 формирования коэффициентов, на первые входы которых подается коэффициент при (k-1)-й степени частичного остатка, полученного на предыдущем шаге.

На второй вход m-го блока 7 формирования коэффициентов подается коэффициент при (m-2)-й степени частичного остатка, полученного на предыдущем шаге, причем m=2,...,k, второй вход первого блока 7 формирования коэффициентов отключен.

На третий вход r-го блока 7 формирования коэффициентов подается коэффициент при (r-1)-й степени полинома модуля, поступающий со входа 4 устройства, причем r=1,...,k. Выход r-го блока 7 формирования коэффициентов представляет коэффициент при (r-1)-й степени частичного остатка. Блок 7 формирования коэффициентов (см. рис. 3) содержит последовательно соединенные умножитель 8 по модулю, вычитатель 9 по модулю и сумматор 10 по модулю.

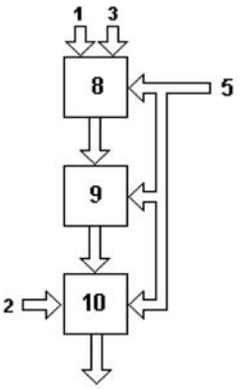


Рис. 3. Блок формирования коэффициентов:
8 – умножитель по модулю; 9 – вычитатель по модулю;
10 – сумматор по модулю

Устройство работает следующим образом. В исходном состоянии на вход 4 поданы коэффициенты полинома модуля $F(x)$, на вход 5 устройства подан код модуля p. Входы 4 и 5 определяют двойной модуль ($F(x)$, p), по которому формируется остаток от полинома $A(x)$. Коэффициенты данного полинома со входа 6 устройства поданы на вторые входы соответствующих умножителей 2 по модулю и определяют значение частичного остатка от соответствующей степени полинома $A(x)$, которое поступит в сумматор 3 по модулю.

Процесс формирования остатка начинается с подачи на первый вход первого блока 1 кода числа «1». В блоке 1 формирования частичных остатков данный код поступает на второй вход второго блока 7 формирования коэффициентов.

В блоке 7 формирования коэффициентов данный код складывается в сумматоре 10 по модулю с результатом, полученным в блоке вычитателя 9 при вычитании значения, поступившего с выхода умножителя 8 по модулю, из значения модуля p. Умножитель 8 по модулю формирует произведение значений, поступающих на его вход со входов 1 и 3 блока 7 формирования коэффициентов.

Полученное значение коэффициента с выхода сумматора 10 по модулю поступает на выход блока 7 формирования коэффициентов, после чего вместе со значениями коэффициентов, сформированными в остальных блоках 7 формирования коэффициентов, поступает на выход блока 1 формирования частичных остатков. С выхода блока 1 формирования частичных остатков значения коэффициентов поступают на вход последующего блока 1 формирования частичных остатков со сдвигом на один разряд в сторону старшего, где с ними осуществляются все вышеуказанные операции, а также на вход умножителя 2 по модулю. В умножителе 2 по модулю значения коэффициентов частичного остатка умножаются на значение коэффициента при степени полинома $A(x)$, от которой вычисляется остаток (на вход i-го умножителя 2 по модулю подается значение коэффициента при (i-1)-й степени полинома $A(x)$, где i=1,...,n) в соответствии с модулем p, поступающим со входа 5 устройства. С выхода умножителя 2 по модулю полученные значения поступают на вход сумматора 3 по модулю, где суммируются со значениями, полученными на предыдущем шаге, в соответствии с модулем p, поступающим со входа 5 устройства. Значения коэффициентов, полученные на выходе n-го сумматора 3 по модулю, являются коэффициентами остатка от полинома $A(x)$ по двойному модулю ($F(x)$, p).

Таким образом, предложенный алгоритм позволяет формировать остатки в расширенных полях $GF(p^n)$ с произвольными значениями p и n от полинома $A(x)$ по двойному модулю ($F(x)$, p).

Литература

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. – М.: Наука, 1981.
2. *Петренко В.И., Кузьминов Ю.В.* Устройство для формирования остатка по двойному модулю. Патент РФ №2299462. Бюллетень №14 от 20.05.07.

Бренд – как механизм достижения высокой популярности

Главный фактор, обуславливающий конкурентный успех - это бренд, поскольку именно он является основой популярности и потребитель готов платить за него больше, чем за какие угодно осязаемые свойства продукции, поскольку именно бренд призван отражать собой самые сокровенные потребности и желания самого целевого потребителя.

Ключевые слова: *управление брендом, популярность, конкурентоспособность, маркетинг, инфокоммуникации.*

Литвинова И.Н.,
Северо-Кавказский филиал Московского технического университета связи и информатики

Brand – as the mechanism of achievement of high popularity

Litvinova I.N.,
North-Caucasian branch of the Moscow technical university relationship and informatics

Abstract

Main factor, defining competitive success – brand since exactly he is a base to popularity and consumer ready to pay for it more, than for whichever palpable characteristic to product since exactly бренд is called to reflect itself the most secret need and desires of the most target consumer.

Keywords: *brand-management, popularity, competitiveness, marketing, telecommunications.*

Для того, чтобы наше путешествие по этапам достижения высокой популярности стало увлекательным, понятным и могло принести практическую пользу читателю важно в самом начале пути определиться с понятием ее основы - брендом. Существует множество трактовок и мнений относительно определения бренда, в бытовом сознании его понятие тесно сопряжено с торговой маркой, или в лучшем случае с имиджем, однако бренд это определенно и не то и не другое, бренд - это их узнаваемость. И для внесения ясности в тематику работы предлагаю близкое мне по духу, авторское определение корпоративного бренда: - это самоидентификация корпоративного имиджа посредством натуральной атрибутики, что и обусловливает его узнаваемость.

В условиях рынка бренд давно стал основой обеспечения популярности и престижа. Для выхода в национальное и тем более в мировое пространство уже не достаточно банальных хороших технических характеристик выпускаемой продукции. Борьба за постоянное повышение качества, несомненно самое гуманное стремление, однако само по себе высокое качество еще не в состоянии обеспечить высокую популярность, поскольку оно является лишь базой для формирования бренда, посредством которого она достигается.

В своих предшествующих работах я приводила основания субъективизма восприятия и критериев качества, основываясь на формулировке, признанной международными стандартами качества ИСО 9000: "Качество – это степень, с которой совокупности характеристик объекта удовлетворяет требования", из которой вытекает, что понятие качества очень индивидуально и субъективно, поскольку требования у всех свои, а уж степень желания их удовлетворить и подавно. И это делает очевидным факт возможности произвольного установления критериев качества, по которым будет оцениваться предлагаемый обществу объект.

На основе детальных маркетинговых исследований социальных состояний формируются предпочтительные для объекта и субъекта брендовой стратегии характеристики и параметры формируемого бренда.

Более того, при разработке критериев качества бренда высокотехнологичной продукции, возможно заложить базисные составляющие для формирования высоконравственной системы ценностей общества.

При этом эффективность бренда определяется его позиционированием, которое заключается в определении места в сознании целевой аудитории и формирование таких образов и атрибутов торговой марки, которые наиболее выгодно отличаются от марок конкурентов, являются для целевого потребителя значимыми, и отвечают его потребительским ожиданиям наилучшим образом.

Сильные бренды построены именно на этом принципе. Например престижно ездить на Lexus и Chrysler круто на Lamborghini. Это уже не просто качественные торговые марки - это бренды, и сформированы они не случайным образом, а с помощью тщательно спланированных и скоординированных мероприятий.

Преимущества сильного бренда обусловлены высокой конкурентоспособностью, которая позволяет не только завоевать максимум потребителей, но и вести ценовую политику, предполагающую повышение цены на продукцию "за известное имя". В этом случае потребитель будет готов дополнительно заплатить за желаемый образ и связанные с ним эмоции. Разумеется эмоции должны быть положительными (не будем ориентироваться на нетрадиционных личностей, которые хотят отрицательных ощущений, их мало!).

Взяв на вооружение оптимистичные перспективы, которые кстати при определенных усилиях и конкретных действиях вполне реаль-

ны, рассмотрим основные этапы достижения популярности.

Поскольку обстоятельства жизни компаний различны, то, скорее всего, и стратегии построения сильного бренда у них будут отличаться.

Можно выделить основную программу достижения популярности (этапы, которые являются базовыми при формировании корпоративного бренда) и дополнительную (действия, относящиеся к специфике производства).

Однако необходимо помнить, что формирование сильного бренда — это бесконечный проект. Никогда не наступит момент, который позволит поставить финальную точку и подвести черту. Такой момент и не должен наступить, поскольку остановка будет означать застой, а застой в эпоху стремительного прогресса ведет к деградации. Поэтому считаю, что сильным может быть только актуальный бренд, а его актуализация достигается через постоянное укрепление целевых позиций и усиление психологического влияния.

Основная программа достижения популярности.

Считаю своим долгом отметить труды первых разработчиков стратегии брендинга, их рекомендации отличаются друг от друга, но некоторое сходство прослеживается:

— предложение Скотта М. Дэвиса (книга "Brand asset management"). [1]

— позиция Дэвида Аакера, изложенная в книге "Brand Leadership". [2]

— восемь этапов строительства бренда из лекций Марка Ритсона, [3] крайне успешного практикующего консультанта по брендингу и преподавателя курса бренд-менеджмента в London Business School.

На основе их опыта становится возможным предложить этапы основной программы, которая с соответствующей адаптацией может быт применена на предприятиях различных отраслей деятельности и в том числе инфокоммуникационных.

Этап 1. Определение цели.

Руководству и ядру рабочей группы, обладающим знаниями о стратегических целях (миссии) компании, необходимо четко определить, каковы стратегические цели бренда. Эти цели удобнее всего формулировать в контексте параметров: осведомленности, накопленного знания и восприятия.

Этап 2. Планирование проекта.

Как и в любом деле, прежде чем начать действовать, необходимо узнать не только цель, но и возможные ограничения, с которыми фирма можете столкнуться, в ходе выполнения проекта, доступные ресурсы, сроки, определить ответственных и исполнителей.

Этап 3. Анализ реального состояния бренда (т.е. представлений о нем в сознании целевого сегмента)

Для того чтобы куда-то добраться, важно понять, где находишься сейчас, или, говоря математически, для того, чтобы нарисовать вектор, недостаточно знать точку конца, надо знать и точку начала. Поскольку бренд - это убеждения, существующие в сознании окружающих, то для того, чтобы понять его реальное состояние, надо провести исследование всех сегментов целевой аудитории.

Этап 4. Анализ соответствия реального состояния бренда желаемому

На данном этапе необходимо спуститься с сияющих небес мечты в прозаическую реальность и посмотреть, насколько ваш живой и непричесанный бизнес может сойти за прекрасного принца.

В долгосрочной перспективе невозможно полностью скрыть несоответствие реального имиджа компании желаемому. И по этому, в ряде случаев гораздо разумнее будет исправить не только формы подачи цели, а свою реальную работу. Если бренд в глазах клиентов выглядит недружелюбным (а дружелюбность и позитивность необходимы для достижения стратегического успеха), то следует натренировать сотрудников, откорректировать продукцию, наладить коммуникации и организовать политику фирмы так, чтобы соответствовать требованиям.

Этап 5. Анализ конкурентов.

Чтобы создать сильный бренд, важно отстроиться от конкурентов. Поскольку соперника надо знать в лицо, следует выявить:

— цели брендинга конкурентов (к какому имиджу они стремятся);

— насколько системно и целенаправленно фирмы-конкуренты занимаются строительством брендов (дееспособна ли армия соперника и велика ли вероятность, что ее цели будут достигнуты);

— проблемы (хотя бы примерно), с которыми конкуренты сталкиваются, чтобы можно было представить вектор их дальнейшего движения.

Этап 6. Разработка стратегии развития бренда

В зависимости от того, насколько сильно различаются желаемое (этап 1,) и реальное (этап 3) состояния бренда, можно понять, какова вероятность успешно реализовать свои цели. стратегия включает ряд элементов:

— позиционирование бренда;

— описание сути бренда (brand essence) и разработка правил создания стандартных дизайнов и текстов (бренд-бук);

— разработка процедур и требований к сохранению, развитию и мониторингу бренда;

— разработка плана конкретных действий.

Этап 7. Выполнение стратегии. Интегрированные маркетинговые коммуникации, организационные изменения в компании

На этом этапе осуществляются все те действия, которые описаны в стратегии (этап 6, пункт "Разработка процедур и требований к сохранению, развитию и мониторингу бренда").

Этап 8. Мониторинг бренда

Для того чтобы регулярно исследовать состояние бренда и следить за собственным прогрессом, нужно очень хорошо понимать, что и зачем делаем. На этом этапе окупятся усилия, направлявшиеся на разработку целей бренда и формулировку их в конкретных измеримых терминах. К сожалению, требования к исследуемым параметрам не позволяют вкладывать в мониторинг скромные средства.

Приведенная программа действий включала только самые необходимые этапы, которые, скорее всего, подойдут любой компании. Однако если у организации есть особенности, то ей придется включить в план действий некоторые элементы "произвольной программы". Примеров особенностей может быть много, я приведу те, которые имеют место на предприятиях связи.

Дополнительная программа

1. Рынок инфокоммуникационных услуг достаточно сложен и в период обострения кризиса - 2009-10 гг. претерпел множество структурных и технологических изменений. В этой связи Институт экономических стратегий Отделения общественных наук РАН традиционно осуществляет постоянный мониторинг уровня стратегического потенциала. На основе программного комплекса "Стратегическая матрица компании" ежегодно строится рейтинг участников рынка телекоммуникаций.

Профиль рынка с его основными участниками, построенный на базе главных стратегических показателей, дает полное представление о важнейших событиях и тенденциях в отрасли. Данный факт накладывает на предприя-

тия связи обязанности постоянного контроля и улучшения основных показателей своей работы.

2. Инфокоммуникационные услуги относятся к технологически сложным и постоянно изменяющимся. Запросы потребителя тоже высокоизменчивы, поскольку развитие отрасли связи в условиях глобализации повышает его осведомленность в части характеристик и условий предоставления услуг связи в мировом информационном пространстве. Получается, что потребитель много знает и поэтому тоже хочет. В этом аспекте предприятиям связи нельзя отставать не в качественной, не в психологической части наполнения своего бренда, иначе любое промедление может повлечь за собой утечку клиентуры в сторону конкурентов.

3. Пакет основных услуг ведущих компаний связи по своей сути и условиям предоставления очень схож, а это означает, что и целевой потребитель тоже в одном регионе один и тот же. Невозможность четкой координации рыночных сегментов одного региона по разным предприятиям связи обостряет конкурентную борьбу. Эта проблема частично может решаться на полуофициальном уровне методом согласования ряда основных условий предоставления услуг, а масштабно для построения сильного бренда просто необходимо специфическое отличие от конкурентов, способное обеспечить его уникальность.

4. Как видно из вышеизложенного, для того, чтобы следовать даже основным канонам управления брендом в инфокоммуникациях, необходимо постоянно осуществлять множество процедур, которые обычно обходятся не дешево. Предприятия связи должны быть готовы, что их брендовый бюджет должен быть существенным и показательным примером этого служит бренд МТС признанный самым дорогим в рейтинге самых ценных российских брендов Best Russian Brands-2010. Перечень опубликовало международное агентство Interbrand. Как сообщили РИА PrimaMedia в Дальневосточном филиале ОАО "МТС", бренд компании оценен в 7,753 млрд. долл.

Наряду с рассмотрением этапов формирования сильного бренда считаю обоснованным уделить особое внимание эффективности дистрибуции бренда, от которой во много зависит успех проекта. Тем более раз уж мы коснулись инфокоммуникационных брендов, здесь я усматриваю некоторые особенности, которыми кстати, можно выгодно воспользоваться.

Средства массовой информации и Интернет круглосуточно обрушивает на нас поток пропаганды зачастую чужих брендов, ориентированных на примитивное сознание обывателя. Рекламные ролики, плакаты, завлекаловки и "желтый" глянец, изобилующие примитивными сюжетами и придурковатыми персонажами часто оскорбляют нас дешевизной своего наполнения. Конечно я не берусь судить за всю страну и если уж такие формы PR используются отечественными производителями, нужно полагать, что они имеют реальную эффективность, ведь некрасивая реклама еще не значит неэффективная. Возможно этим производителям достаточно того обширного сегмента потребителей, который глотает примитивные наживки и такие дистрибьюторы брендов предпочитают не заморачиваться на интеллектуальном развитии своего народа. И все-таки даже если некрасивая реклама является эффективной, она все равно остается некрасивой и потому не только не ускоряет, а напротив угнетает экономическое и культурное развитие общества.

В процессе разработки концепции продвижения бренда происходит выбор каналов коммуникации в рамках, определенных планом и стратегией маркетинга, способов продвижения бренда, при помощи которых коммуникационное послание будет доноситься до целевой аудитории. Осуществляется отбор каналов коммуникаций в соответствии со спецификой позиционирования бренда и его креативной концепцией, определяются цели, задачи и роли каждого из выбранных каналов коммуникации, разрабатывается стратегия их использования и взаимодействия.

При этом подчеркиваю, наличие широкого многообразия каналов коммуникаций, существующих в современном обществе, которые дают огромные возможности выхода как в локальное, так и в глобальное информационное пространство. Эти каналы необходимо, по возможности максимально активно использовать в целях пиара высокотехнологичных брендов, а вместе с ними и инновационных ценностей, так недостающих современному обществу. И здесь у предприятий связи в наличии имеются огромные преимущества, поскольку именно им как никому другому максимально открывается доступность использования инфокоммуникационных каналов.

Однако интенсивность еще не определяет эффективность, брендинг дело тонкое и подходить к нему нужно со всей серьезностью и осторожностью во избежание не только отсутствия положительного результата, но и негативных, порой непредсказуемых последствий. Механизмам и уникальным нюансам формирования корпоративных и персональных брендов посвящена широкая область знаний, требующая отдельного изучения в других трудах. В своей статье "Эффективность дистрибуции образовательного бренда" я подробно описала наиболее распространенные недоработки в процессе дистрибуции брендов и их последствия. Могу только резюмировать, что роль каналов коммуникации в процессе PR-поддержки строительства сильного бренда весьма высока и отводить выбору этих каналов второстепенное место неразумно и часто опасно для репутации бренда.

Для целевой аудитории и общества эффективность состоит в повышении их культурного уровня и интеллектуального потенциала. Обществу нужны кумиры и ориентиры. Развитие личности и формирование ее системы ценностей происходит в имеющемся информационном пространстве. Если в нем мало сведений об интеллектуальных продуктах, то этот пробел с удовольствием (что и происходит) займут далекие от нравственности информационные потоки, и тогда уже под их влиянием будут формироваться идеалы нашего народа.

Для инфокоммуникационных компаний сильный бренд — это прежде всего повышение рыночной конкурентоспособности и финансовой устойчивости, а высокоразвитая, прогрессивная связь во многом способствует повышению производственной активности в государстве.

Литература

1. *Дэвид А. Аакер, Эрик Йохимштайлер* Brand Leadership: The Next Level of the Brand Revolution (Бренд-лидерство: новая концепция брендинга) Издат.: Издательский дом Гребенникова, 2009 .

2. *Настасья Савина* "Великая стройка бренда. Этапы большого пути". www.e-xecutive.ru.

3. *Скотт Дэвис* "Brand Asset Management" (Управление автивами торговой марки). — СПб., Питер, 2005.

4. Труды международной научно-практической конференции СКФ МТУСИ "ИНФОКОМ-2010". — Ростов н/Д , 2010.

5. *Ritson M.* http://www.marketingritson.com.

WiMax integration in russian broadband access market

The paper considers WiMAX 4G technology as an alternative to the Wi-Fi technology as well as potentials and prospects of its integration in the telecommunications services market in Russia.

Keywords: *broadband, high-speed fixed and mobile broadband, bandwidth, new services, high customer satisfaction.*

Miachin S.S., Svetlichnaya N.O.,
North-Caucasian branch of the Moscow technical university relationship and informatics

WiMAX is the first 4G technology to meet the increasing demand for the mobile Internet. WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that provides fixed and mobile Internet access. The current WiMAX revision provides up to 40 Mbit/s with the IEEE 802.16m update expected to offer up to 1 Gbit/s fixed speeds. WiMAX refers to interoperable implementations of the IEEE 802.16 wireless-networks standard, in similarity with Wi-Fi, which refers to interoperable implementations of the IEEE 802.11 Wireless LAN standard (ratified by the Wi-Fi Alliance). Mobile WiMAX is the WiMAX incarnation that has the most commercial interest today and is being actively deployed in many countries. Mobile WiMAX is also the basis of future revisions of WiMAX.

WiMAX and Wi-Fi are frequently compared and confused because both are related to wireless connectivity and Internet access. However they differ in many aspects.

WiMAX is a long range system, covering many kilometres, that uses licensed or unlicensed spectrum to deliver connection to a network, in most cases the Internet.

Wi-Fi uses unlicensed spectrum to provide access to a local network.

Wi-Fi is more popular in end user devices.

Wi-Fi runs on the Media Access Control's CSMA/CA protocol, which is connectionless and contention based, whereas WiMAX runs a connection-oriented MAC.

WiMAX and Wi-Fi have quite different quality of service (QoS) mechanisms.

Both 802.11 (which includes Wi-Fi) and 802.16 (which includes WiMAX) define Peer-to-Peer (P2P) and ad hoc networks.

Although Wi-Fi and WiMAX are designed for different situations, they are complementary. WiMAX network operators typically provide a WiMAX Subscriber Unit which connects to the metropolitan WiMAX network and provides Wi-Fi within the home or business for local devices (e.g., Laptops, Wi-Fi Handsets, smartphones) . This enables the user to be able to use the WiMAX network.

3G and Wi-Fi have whetted consumers' appetites for mobile data. Moreover, as mobile data networks become increasingly congested, WiMAX can affordably deliver two to four times the performance of today's 3G solutions, with the ability to scale to 10 times the performance with 802.16m, the next version of the IEEE 802.16 standard upon which WiMAX is based. This is great news for multi-megabit video, sending and receiving pictures and large files, and social media users.

WiMAX is being deployed around the world and offers low-cost connectivity with the added bonus of mobility. Additionally, given the relatively low costs associated with the deployment of a WiMAX network (in comparison with 3G, HSDPA, xDSL, HFC or FTTx), it is now economically viable to provide last-mile broadband Internet access in remote locations.

Key members of the computing, telecommunications, and Internet industries are delivering what is considered to be disruptive technology for the connected world-WiMAX-and enjoying some common benefits:

One unifying technology for both mature and emerging markets.

Affordable connectivity for multi-megabit fixed and mobile broadband across cities and countries through a variety of devices.

Providing a wireless alternative to cable and DSL for "last mile" broadband access.

Ease and speed of deployment, reducing time-to-market, and yielding faster return on investment.

New video and social media services (data, telecommunications (VoIP) and IPTV services) for differentiated offerings.

Providing a source of Internet connectivity as a part of a business plan.

High customer satisfaction to retain and grow subscribers .

WiMAX offers significant speed, loads of capacity, and lower prices. Currently, there are more than 500 Fixed and Mobile WiMAX trials and commercial deployments in 146 countries, including Russia. Integration of the mobile WiMAX in Russia as well as in many other countries is complicated due to the impossibility to release the used frequencies and employ them for the Internet connectivity. At present the devices manufactured for WiMAX networks can support three main frequency bands: 2,5 - 2.7, 3.4 - 3.6 and 5 - 6 GHz. Splitting the standard into these ranges was made to simplify the process of licensing in different countries. However, the frequency range of 3.5 GHz is not free in Russia. It is used by ground and satellite wireless systems including military ones. The frequency range of 2,5-2,7 GHz is used by the satellite television. Thus the only available range suitable for WiMAX standard is 5,725-5,850GHz.

According to the forecasts of analysts the first commercial mobile WiMAX networks in Russia have to appear in 2011.

Scartel's Yota service delivers mobile broadband services using cutting-edge 4G Mobile WiMAX technology. In fact, Scartel is the largest Mobile WiMAX in Russia covered a population of over 23 million in 2009 , launched 15 new cities in 2010 and plans to expand internationally. It offers Internet access along with rich media mobile services (music and video on demand, IPTV, and so on) at speeds up to 10 Mbps per user device. Before the Yota service became available, mobile Internet access in Russia was slow, expensive, and not widely deployed. By contrast, after just six months of commercial operations, Yota reached its 250,000th active commercial user, passing its breakeven point thanks to more than 2,300 subscribers added per day to its WiMAX networks in Moscow, St. Petersburg, and beyond. Due to robust base station provisioning, current average data consumption of a Yota subscriber is in excess of 10 GB per month, more than twice the average use of wired Internet subscribers in Moscow and many times the capacity limits of 2G and 3G data services. Scartel's ultimate goal is to deploy networks in more than 40 Russian cities, beginning in those with populations over 1,000,000 and moving to those with populations over 500,000. A wide range of Mobile WiMAX access devices can access the Yota service, including:

Notebooks: In 2009, Yota saw more than 65 notebook models from six PCs manufacturers introduced in its markets.

Mobile Phones: The HTC MAX* 4G is the world's first dual-mode global system for mobile communication (GSM) and Mobile WiMAX handset.

USB Modems: The 4G Samsung USB dongle provides simple access to the 4G Internet from a PC or laptop.

IAD: The ASUS Mobile WiMAX Wi-Fi Center offers fast wireless Internet, VoIP, and local networks for home and office.

Express Cards: The Samsung Express Card 4G offers a compact 4G Internet for people on the go.

The IEEE 802.16m standard is the core technology for the proposed WiMAX Release 2, which enables more efficient, faster, and more converged data communications. WiMAX Release 2 will provide strong backward compatibility with Release 1 solution. It will allow current WiMAX operators to move easily from their Release 1 solutions to Release 2. It is expected that the WiMAX Release 2 will be available commercially in the 2011-2012 period.

References

1. *K. Fazel and S. Kaiser,* Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX, 2nd Edition, John Wiley & Sons, 2008.

2. *M. Ergen,* Mobile Broadband – Including WiMAX and LTE, Springer,NY,2009.

3. WiMAX Forum (http://www.wimaxforum.org/home).

4.(http://www.ciscosystems.com/web/about/ac123/ac147/archieved_issues/ipj_112/112_wimax.html).